VIII Ciclo de Conferencias
UPM – TASSI

Aplicaciones de la Biometría a la Seguridad

Carmen Sánchez Ávila

Grupo de Biometría, Bioseñales y Seguridad
Centro de Domótica Integral (CEDINT)
Universidad Politécnica de Madrid
Email: carmen.sanchez.avila@upm.es
Web: http://www.gb2s.es/

Índice

1. Introducción a la Biometría
2. Principales sistemas biométricos basados en:
   - Huella dactilar
   - Iris
   - Mano
   - Cara
3. Algunas aplicaciones de la Biometría
4. Problemas abiertos y tendencias futuras

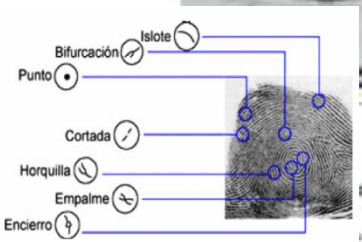
Biometría

- **Objetivo: la identificación de una persona mediante sus características biofísicas o de comportamiento**
- **Técnicas biométricas más conocidas:**
  - Huella dactilar
  - Características del ojo: iris y retina
  - Geometría de la mano e imagen vascular
  - Características faciales
  - Composición química del olor corporal
  - Líneas de la mano

  - Escritura manuscrita
  - Voz
  - Tecleo
  - Gesto y movimiento corporal

Biometría: técnicas biométricas más conocidas

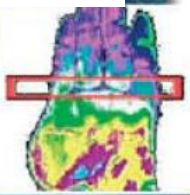
Reconocimiento facial

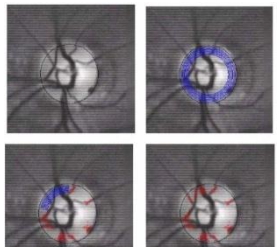


Reconocimiento de huellas dactilares

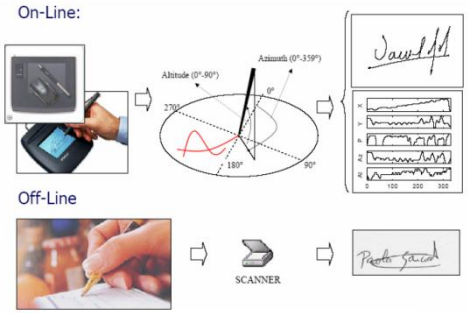
Reconocimiento de iris

cimiento de
ca de tecleo

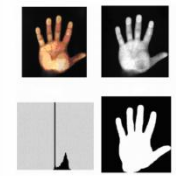


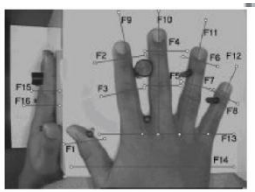


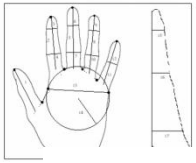
Reconocimiento de retina



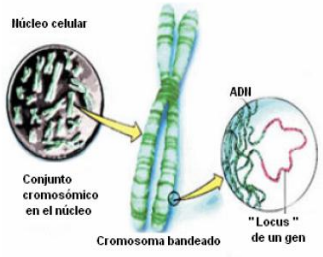
Reconocimiento biométrico de la firma

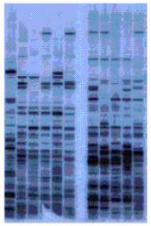


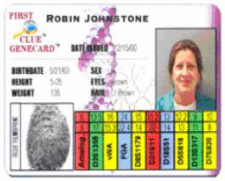




Reconocimiento biométrico de la geometría de la mano





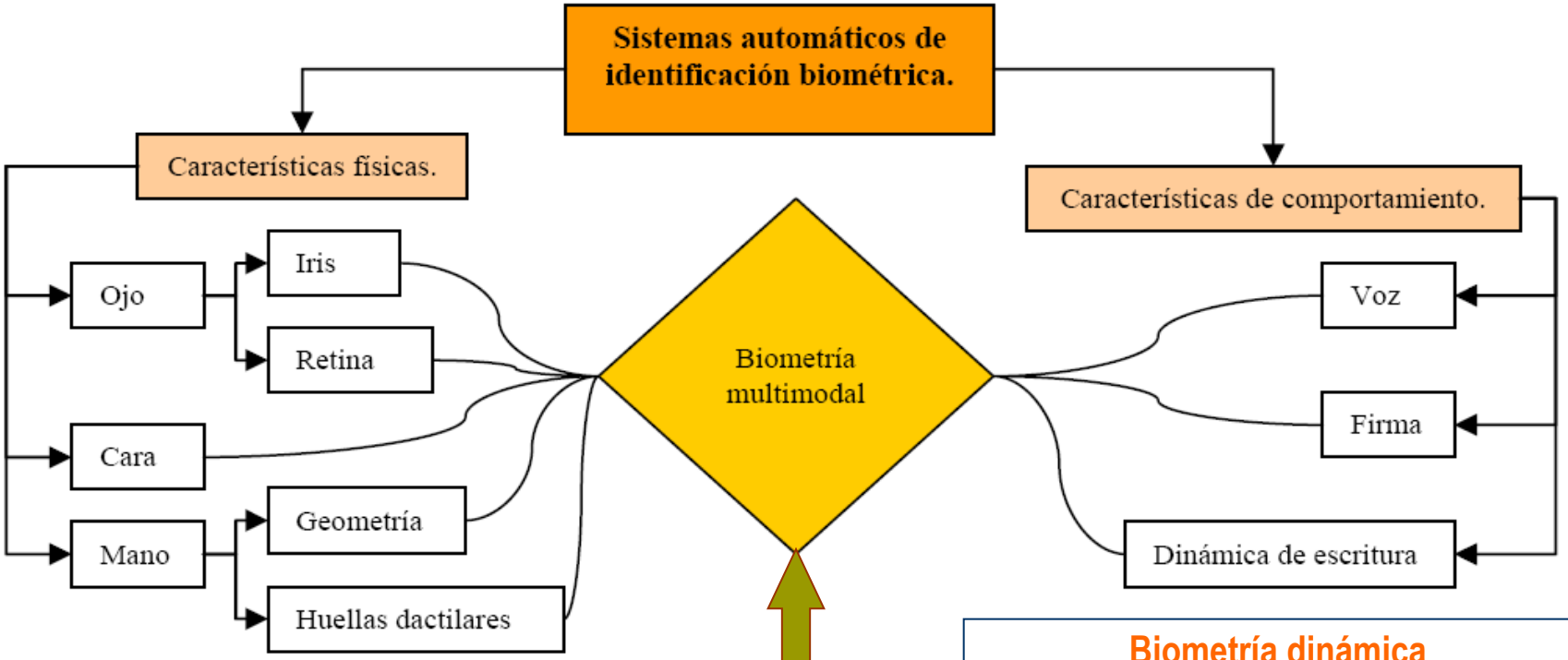


Reconocimiento de ADN

Reconocimiento de voz

Carmen Sánchez Ávila

Biometría



Biometría estática
Medida de rasgos físicos de la persona

Biometría dinámica
Medida de diferentes comportamientos de cada persona

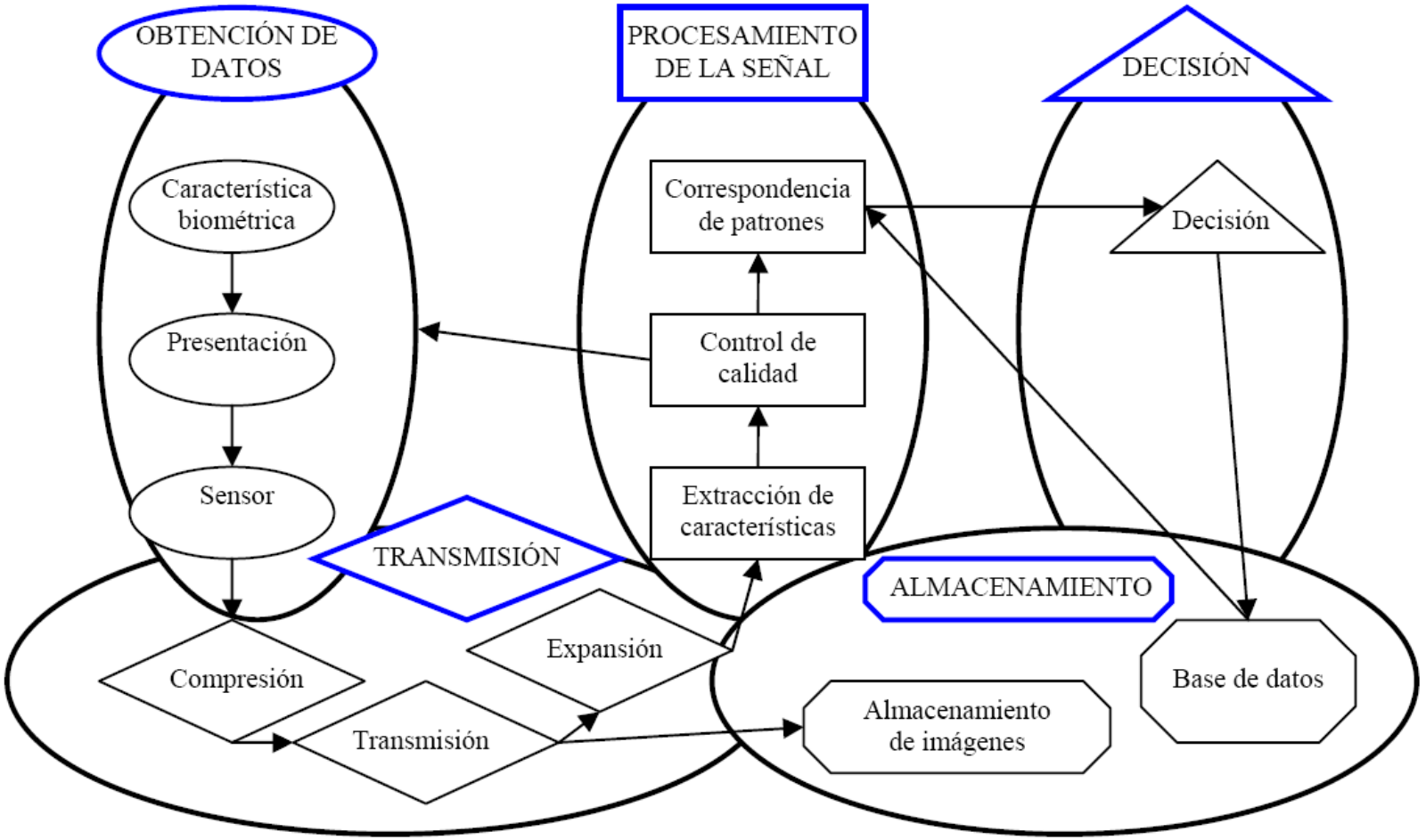
Biometría multimodal
Combinación de medidas, tanto físicas como de comportamiento

Biometría

- **Los requisitos básicos que deben reunir las características biométricas son:**
  - **Universalidad**: todos los usuarios la tienen
  - **Singularidad o univocidad**: carácter distintivo
  - **Permanencia**: en el tiempo y condiciones ambientales diversas
  - **Colectividad**: ha de ser mensurable cuantitativamente
  - **Rendimiento o actuación**: elevado nivel de exactitud
  - **Aceptación**: por parte del usuario
  - **Resistencia a fraude** o usurpación

Biometría

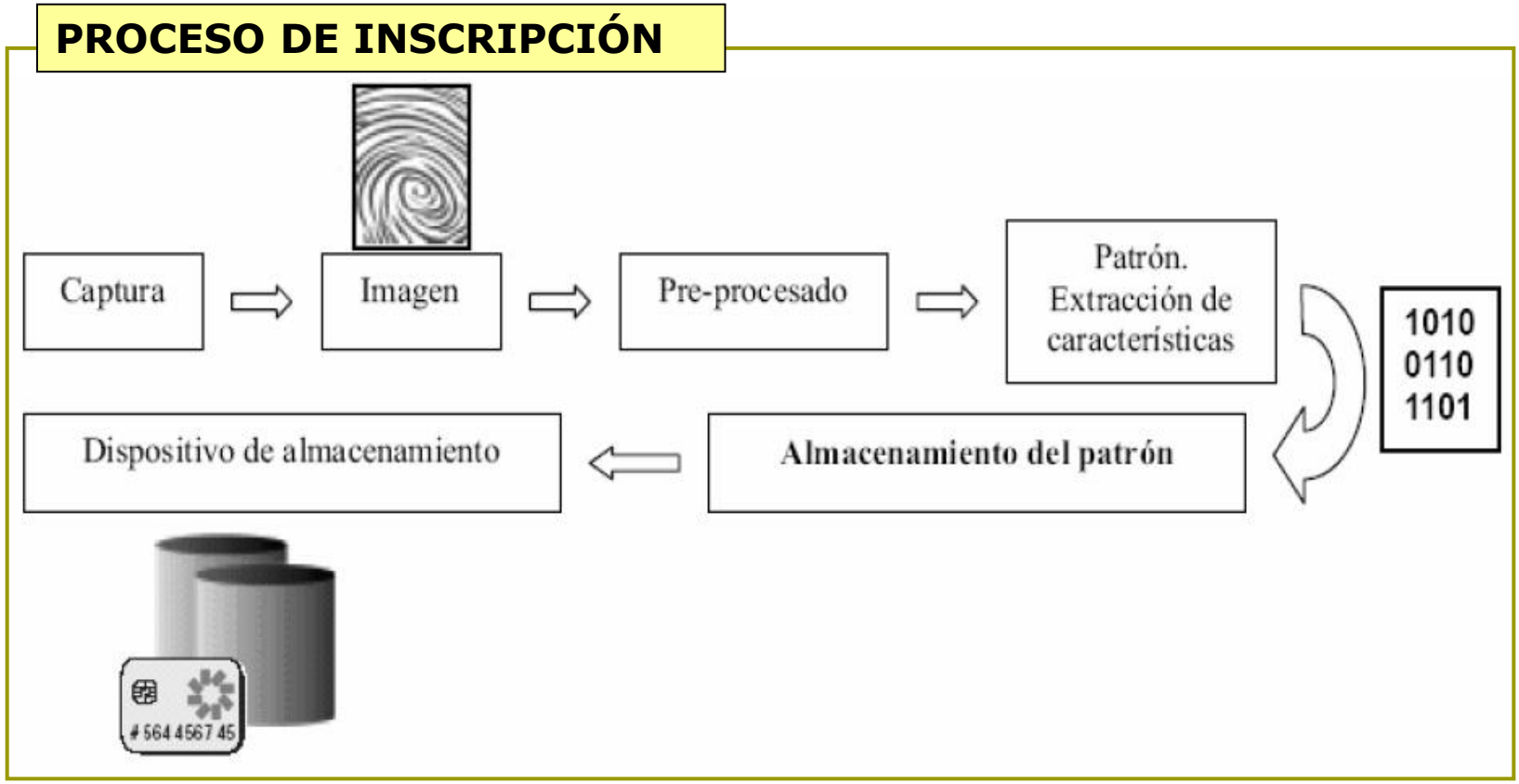
Bloques y etapas de un sistema biométrico



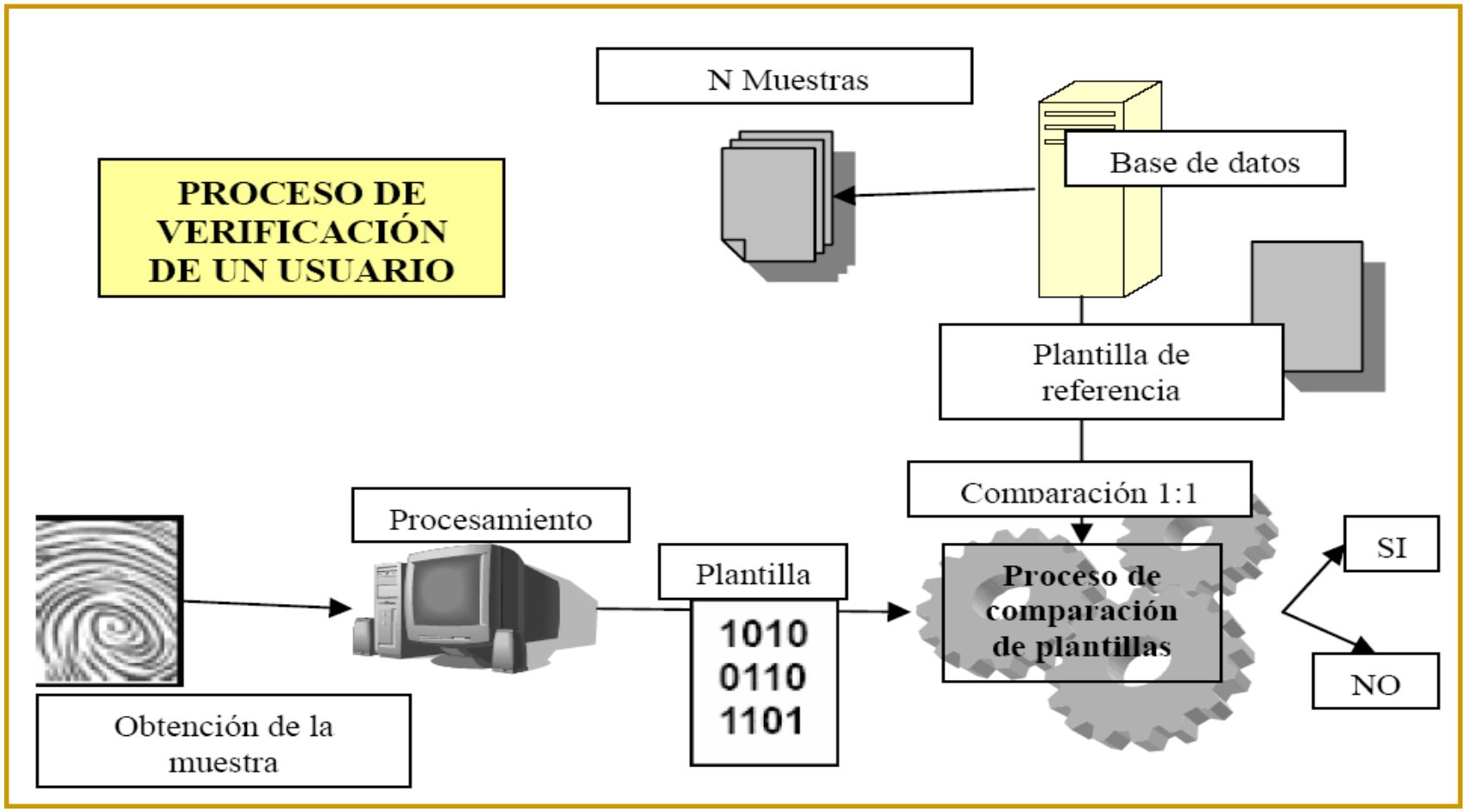
Biometría

- Esquemas de Funcionamiento:
  - **Reconocimiento:** *(¿quién es?)* Se compara la muestra con todos los patrones almacenados de los distintos usuarios del sistema
  - **Autenticación:** *(¿es quién dice ser?)* Se compara la muestra con el patrón del usuario que reclama su identidad.
- Etapas:
  - Captura de los datos biométricos
  - Preprocesado de los datos capturados
  - Extracción de las características propias del usuario
  - Comparación con el patrón almacenado:
    - Clasificador (reconocimiento biométrico): 1 – N
    - Verificador (autenticación biométrica): 1 – 1

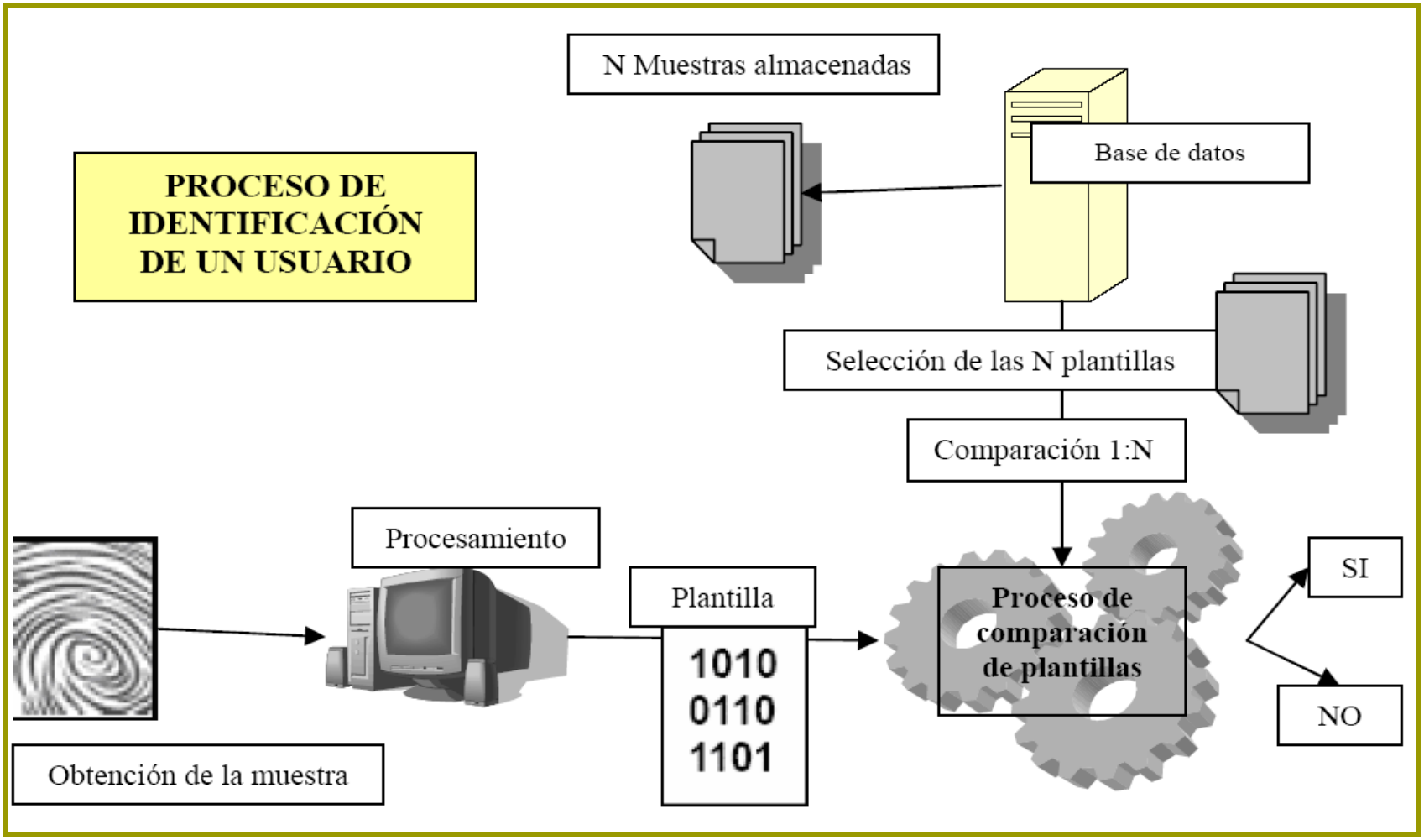
Biometría


PROCESO DE INSCRIPCIÓN
Captura
Imagen
Pre-procesado
Patrón.
Extracción de
características
1010
0110
1101
Dispositivo de almacenamiento
Almacenamiento del patrón
564 4567 45

Biometría


PROCESO DE VERIFICACIÓN DE UN USUARIO
N Muestras
Base de datos
Plantilla de referencia
Comparación 1:1
Procesamiento
Plantilla
1010
0110
1101
Proceso de comparación de plantillas
SI
NO
Obtención de la muestra

Biometría


N Muestras almacenadas
Base de datos
PROCESO DE IDENTIFICACIÓN DE UN USUARIO
Selección de las N plantillas
Comparación 1:N
Procesamiento
Plantilla
1010
0110
1101
Proceso de comparación de plantillas
SI
NO
Obtención de la muestra

Biometría

Característica	*Aceptación del usuario*	*Facilidad de uso*	*Coste*	*Utilidad*		*Estabilidad*	*Intrusismo*	*Fiabilidad*
				Identificación	*Verificación*			
ADN	Baja	Baja	Alto	✓	✓	Alta	Muy alto	Alta
Dinámica de escritura	Alta	Alta	Bajo	✗	✓	Baja	No	Baja
Firma	Media	Alta	Bajo	✗	✓	Media	No	Baja
Geometría de la mano	Media	Alta	Alto	✗	✓	Media	No	Media
Huella dactilar	Media	Alta	Bajo	✓	✓	Alta	Bajo	Alta
Iris	Media	Media	Alto	✓	✓	Alta	No	Alta
Reconocimiento facial	Media	Media	Bajo	✗	✓	Media	No	Media
Retina	Media	Baja	Alto	✓	✓	Alta	Alto	Alta
Voz	Alta	Alta	Bajo	✗	✓	Media	No	Baja

Característica	*Nivel de seguridad*	*Ratio de error*	*Precisión*	*Errores*	*Falso positivo*	*Falso negativo*
ADN	Alto	Sin datos	4	No conocidos.	5	5
Dinámica de escritura	Medio	Sin datos	1	Lesiones de mano, cansancio.	3	1
Firma	Medio	1/50	2	Cambios de escritura.	2	1
Geometría de la mano	Medio	1/500	3	Edad, lesiones varias.	4	2
Huella dactilar	Alto	1/500+	4	Sequedad, suciedad, edad.	5	5
Iris	Alto	1/131000	4	Iluminación inadecuada.	4	4
Reconocimiento facial	Medio	Sin datos	3	Pelo, gafas, edad, iluminación.	3	1
Retina	Alto	$1/10^6$	4	Gafas, lentillas.	5	5
Voz	Medio	1/50	2	Ruidos, ronquera, resfriados…	2	1

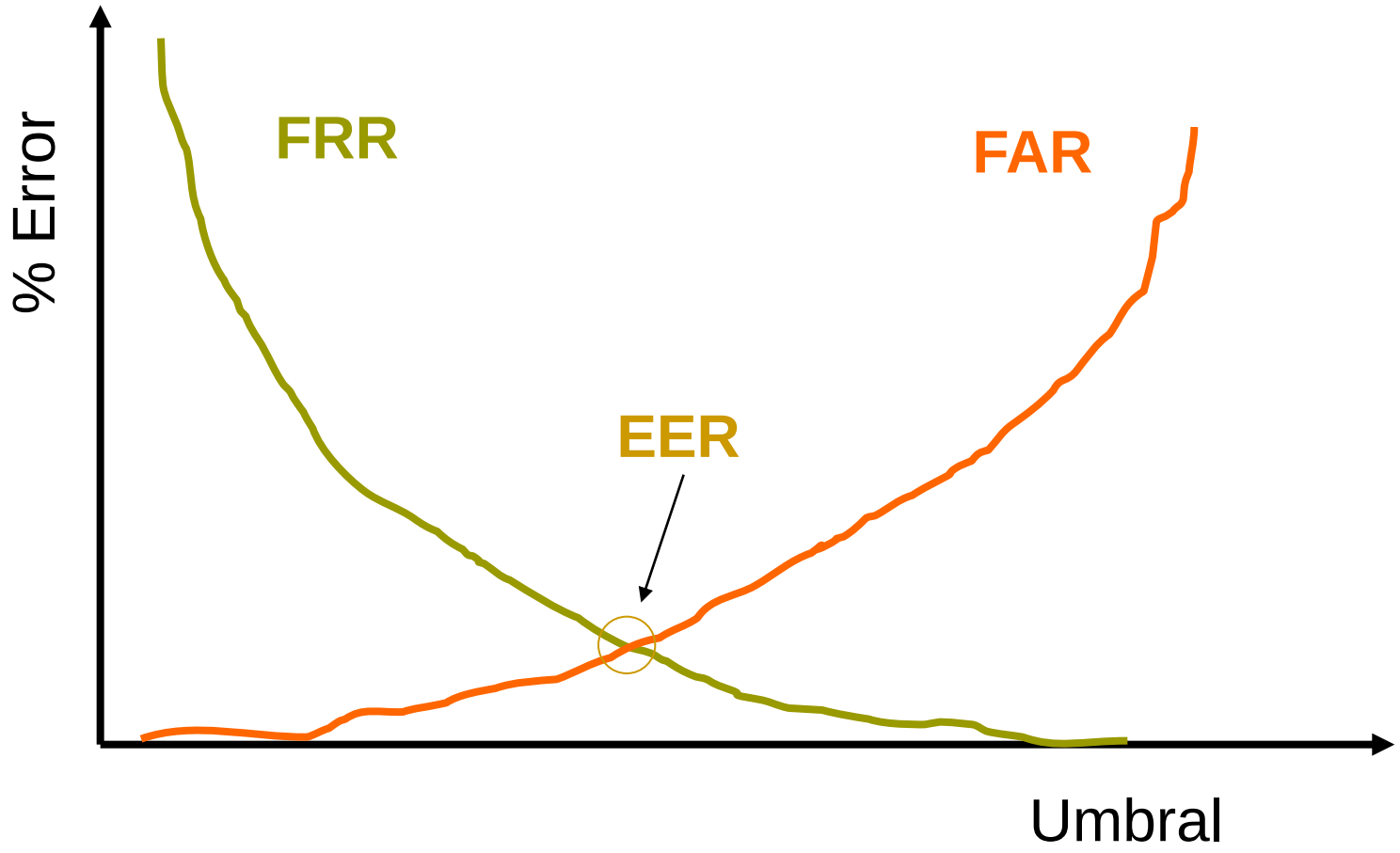
Carmen Sánchez Ávila

Biometría: rendimiento de los sistemas

- **Tasa de falsos positivos TFP (*False Match Rate, FMR*)**
  Proporción de muestras falsamente asignadas a un usuario al que no le pertenecen
- **Tasa de falsos negativos TFN (*False Non Match Rate, FNMR*)**
  Proporción de muestras falsamente rechazadas como pertenecientes al cliente al que pertenecen

- **Tasa de Falsa Aceptación (FAR)**
  Proporción de veces que se acepta a un intruso como usuario del sistema
- **Tasa de Falso rechazo (FRR)**
  Proporción de veces que se rechaza a un usuario legítimo del sistema
- **Tasa de Igual Error (EER)**
  Valor para el que FAR=FRR

Biometría: rendimiento de los sistemas



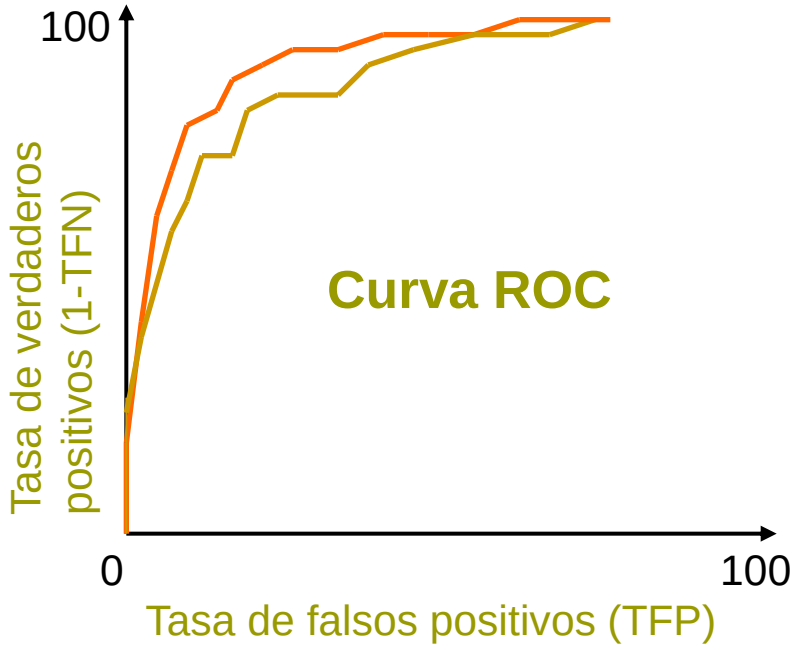
Biometría: rendimiento de los sistemas

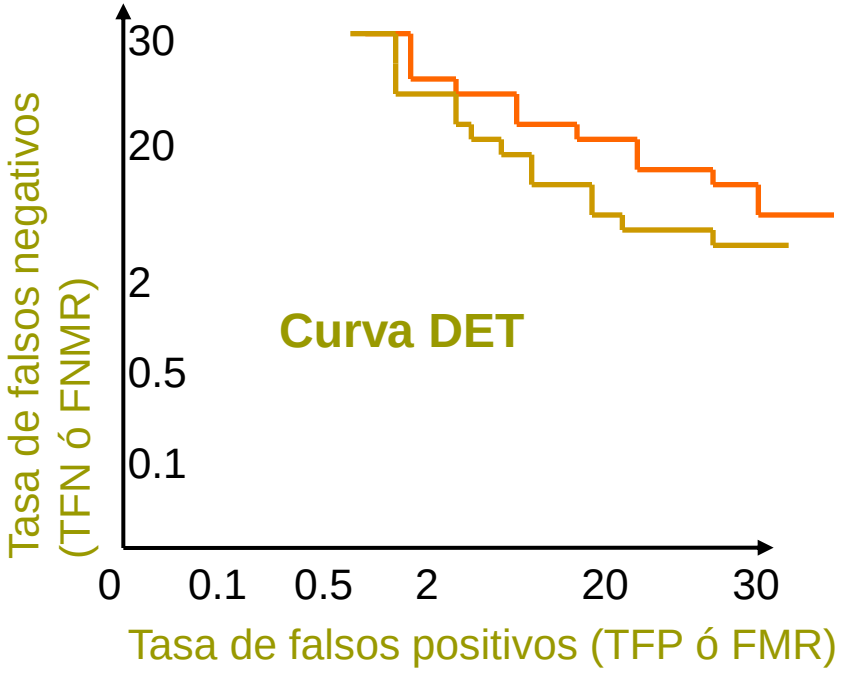
Curva ROC (Receiver Operating Characteristics)

- Muestra la variación de la TFP y al tasa de verdaderos positivos (1-TFN) con respecto a un determinado umbral

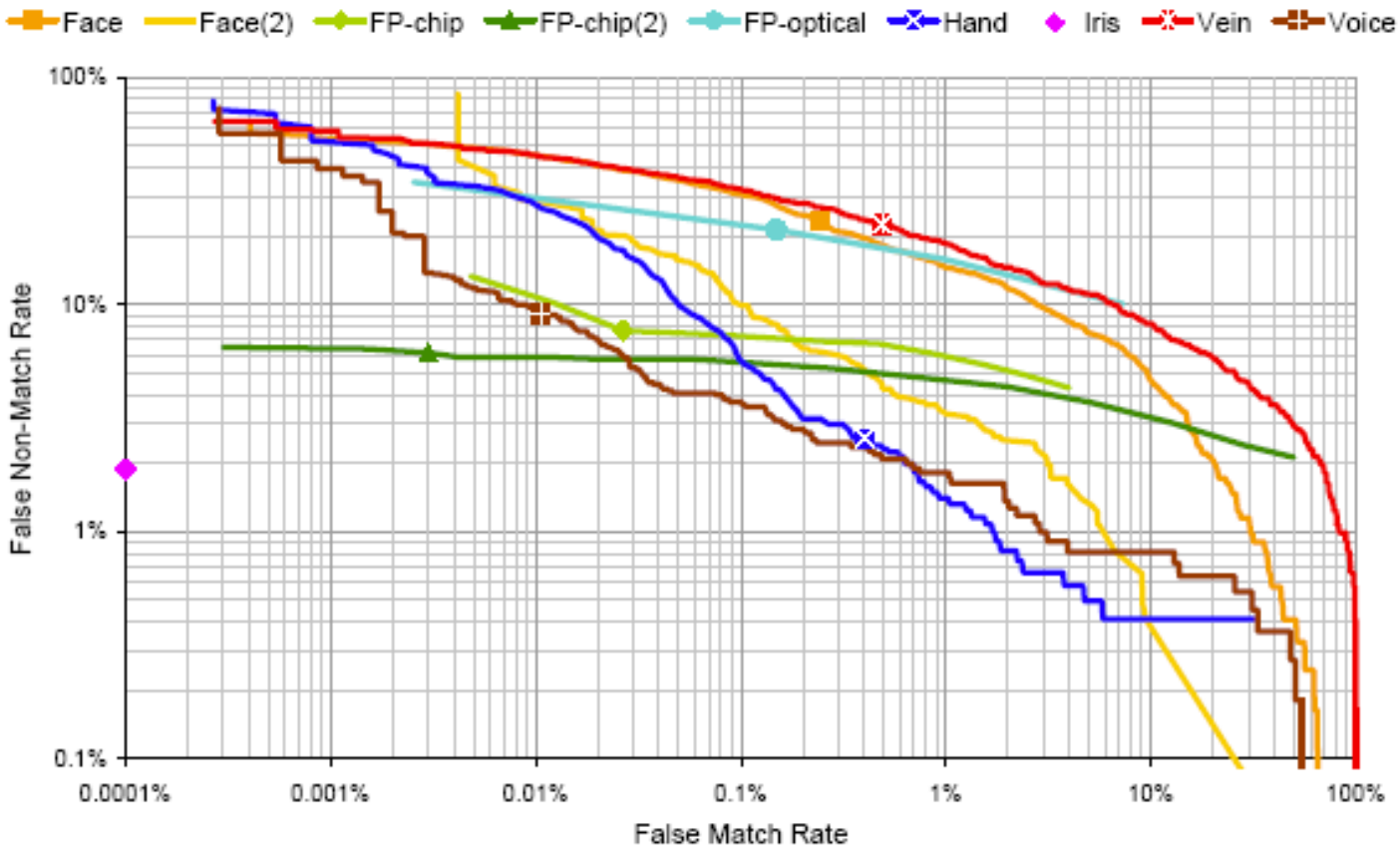
Curva DET (Detection Error Tradeoff)

- Muestra el número de desviaciones normales en la distribución normal estándar correspondiente a las probabilidades de FP y de FN



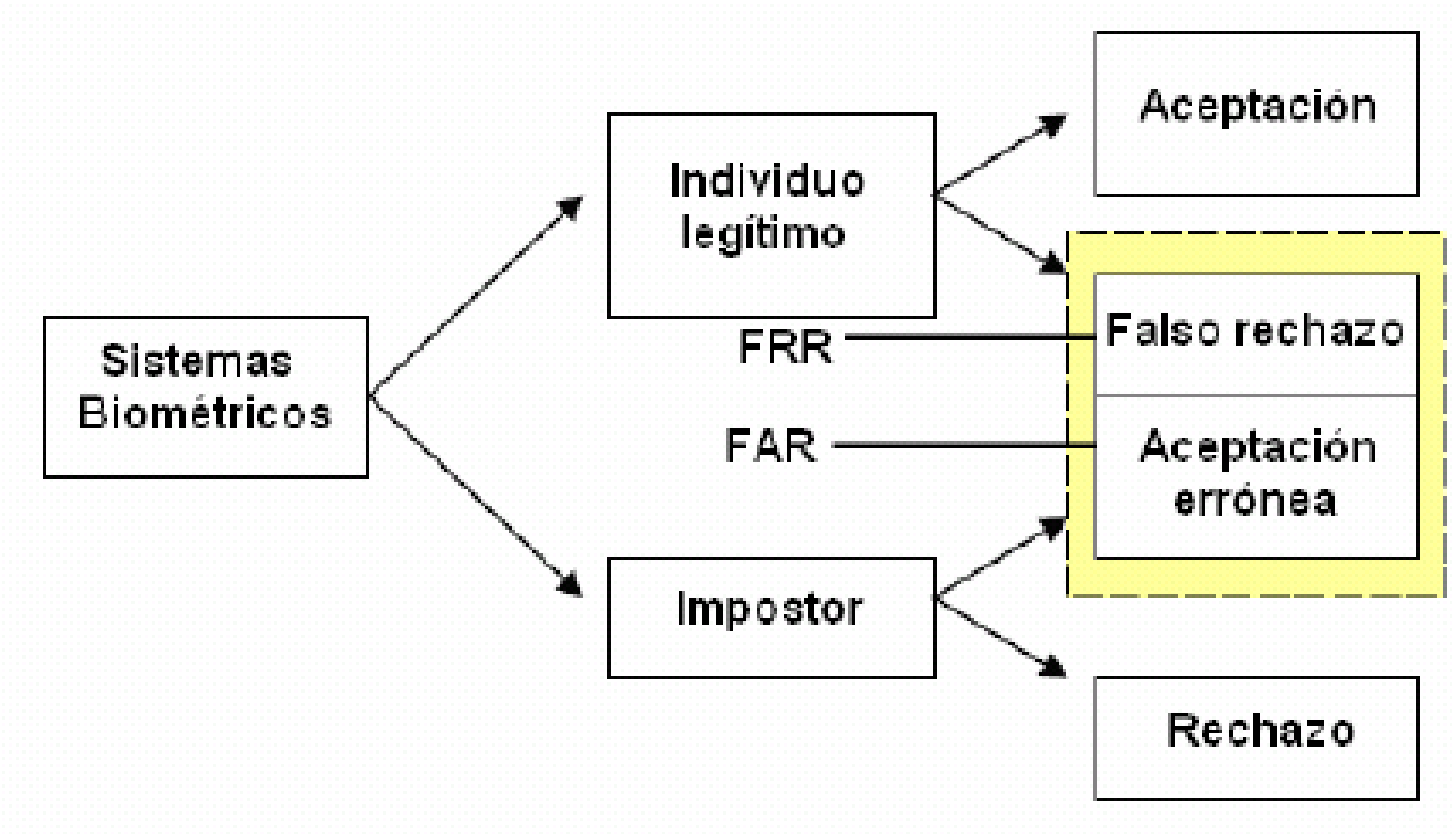


Biometría: rendimiento de los sistemas (curva DET)

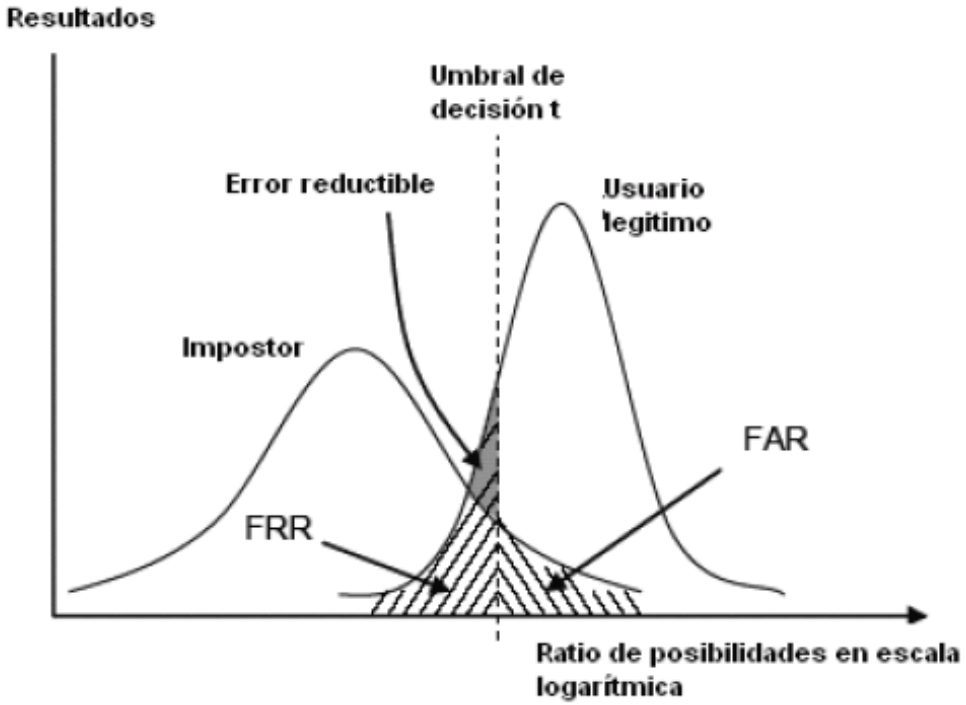


Referencia: T. Mansfield et al., Biometric Product Testing Final Report, Centre for Mathematics and Scientific Computing, National Physical Laboratory, 2002.

Biometría: rendimiento de los sistemas



Biometría: rendimiento de los sistemas



Necesidad de un compromiso en el valor del umbral que haga que los valores tanto de FAR, como de FRR, permitan funcionar al sistema de manera correcta.

↑ Umbral → ↓ FAR & ↑ FRR

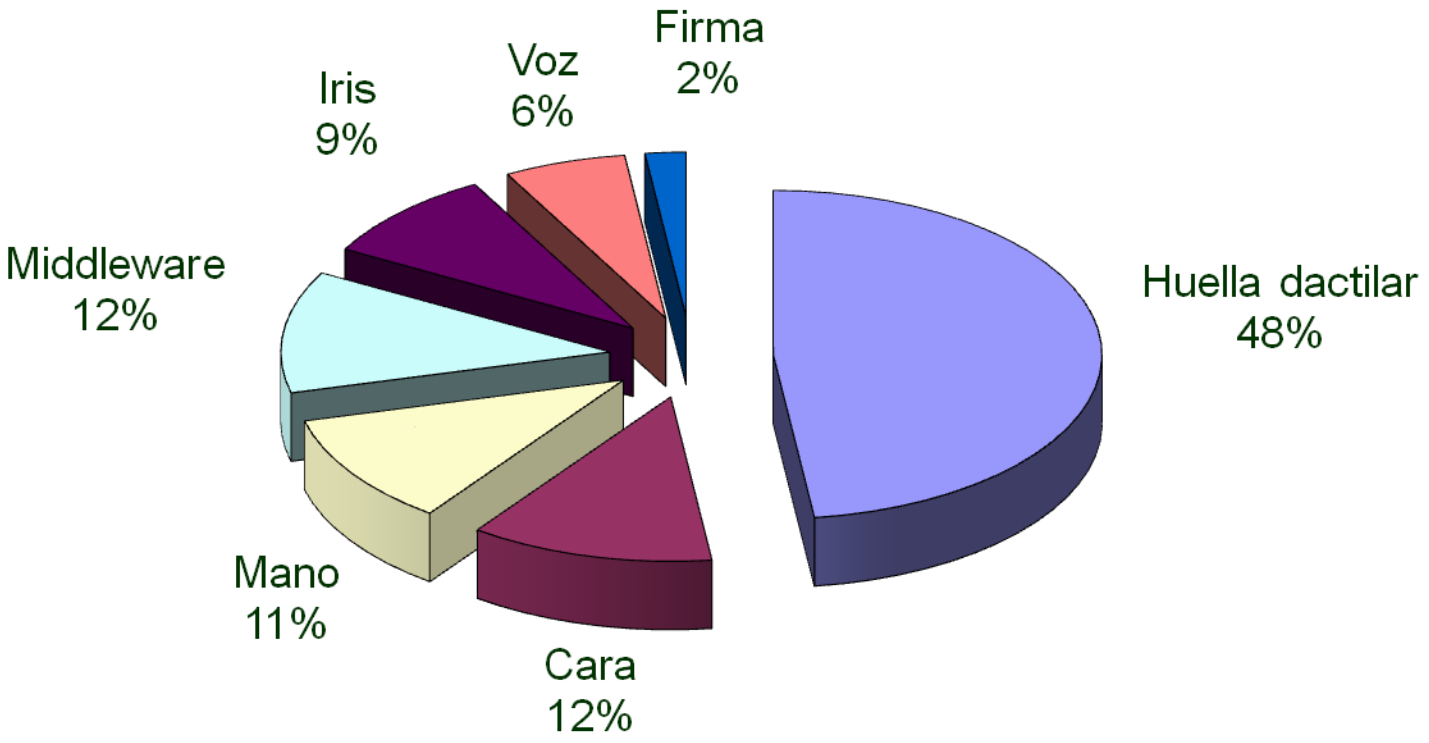
↓ Umbral → ↑ FAR & ↓ FRR

El valor dependerá en gran parte de las necesidades de seguridad de la aplicación en cuestión.

Biometría: evaluación estándar de la tecnología

- Evaluaciones objetivas realizadas por laboratorios independientes con el fin de medir el estado de la tecnología biométrica
- Utilizan bases de datos estándar y generalmente son abiertas
- Ejemplos:
  - FVC (Fingerprint Verification Competition)
    https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx
  - FRVT (Face Recognition Vendor Test)
    http://www.frvt.org/FRVT2006/default.aspx
  - FRGC (Face Recognition Gran Challenge)
    http://www.frvt.org/FRGC/Default.aspx
  - NIST Speaker Recognition Evaluation (voz)
    http://www.nist.gov/speech/tests/spk/index.htm
  - ICE (Iris Challenge Evaluation)
    http://iris.nist.gov/ICE/

Biometría: cuota de mercado en tecnología biométrica



Algunas técnicas biométricas

Carmen Sánchez Ávila

Huella dactilar

Carmen Sánchez Ávila

Huella dactilar: propiedades

- Universalidad (media-alta)
  - Más de un 96% de la población tiene una huella legible
- Univocidad (alta)
  - Incluso gemelos idénticos tienen huellas diferentes
- Permanencia (alta)
  - La huella se forma en la etapa fetal y permanece estructuralmente inalterable a lo largo de la vida
- Rendimiento (alto)
  - Es una de las técnicas biométricas con mejor rendimiento
  - Mayor compromiso entre comodidad y seguridad
- Aceptación (media)
  - La captura de la imagen de la huella no es intrusiva
  - Posee implicaciones legales

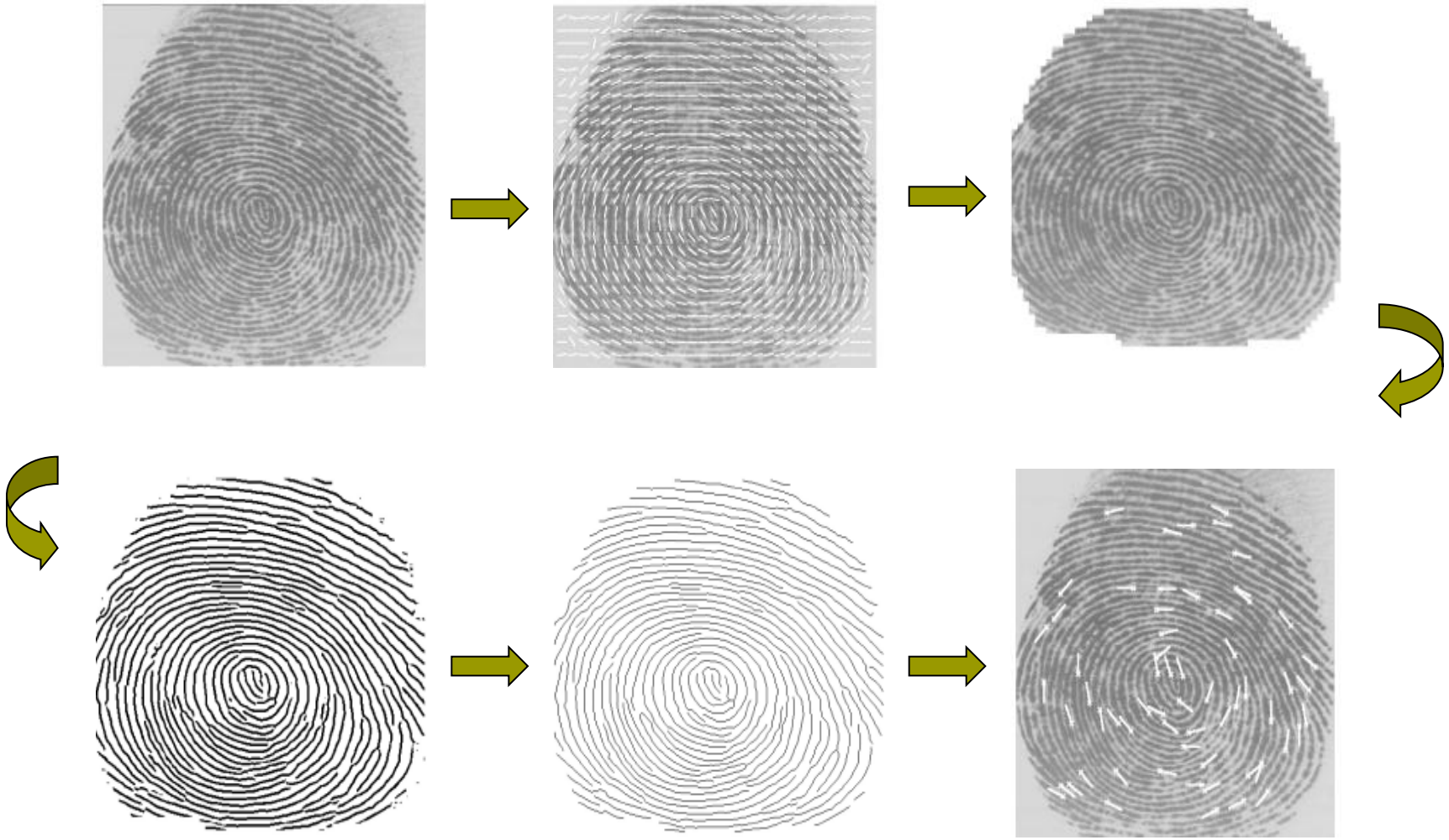
Huella dactilar: paradigmas

- Manual
  - Consiste en la inspección visual, de texturas y de minucias, además de la experiencia del experto
- Técnicas basadas en imagen
  - Utilizan sólo la apariencia visual de la imagen
  - Es necesario almacenar la imagen completa
- Métodos basados en texturas
  - Tratan la huella como una imagen de texturas orientadas
  - Menos preciso que las técnicas basadas en minucias
- Técnicas basadas en minucias
  - Utilizan las posiciones relativas de las minucias
  - Es el método más conocido y preciso

Huella dactilar: técnica basada en minucias

- Preprocesado
  - Estimación del campo de orientación y realce de la imagen
  - Binarización (de 8 bits/píxel a 1 bit/píxel)
  - Extracción de la región de interés (ROI)
  - Adelgazamiento y depuración de la imagen
- Extracción de características: minucias
- Establecimiento del patrón de huella: datos que corresponden a la disposición de las minucias (300 bytes)
- Etapa de comparación

Huella dactilar: técnica basada en minucias



Huella dactilar: técnica basada en minucias

- Se convierten todas las minucias (modelo y muestra) a coordenadas polares. Centro: la minucia de referencia
- Se representan (patrón y muestra) mediante cadenas de puntos

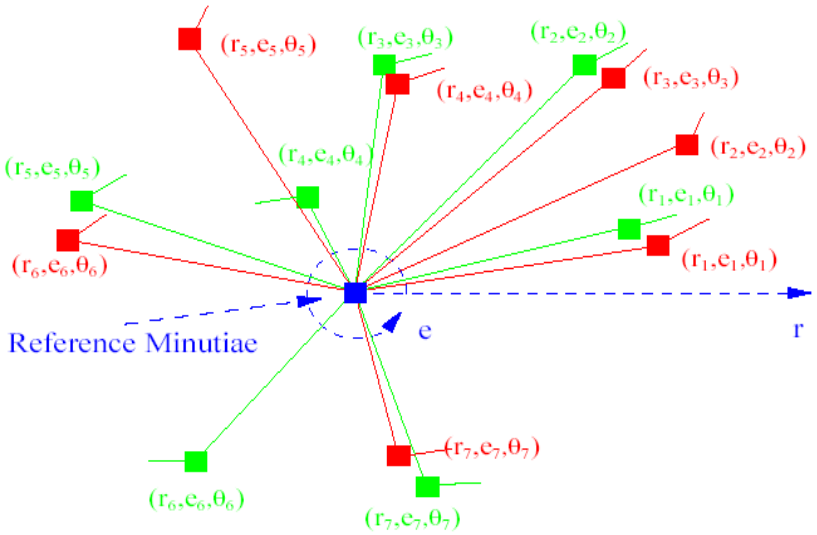
$$P_p = \left(\left(r_1^P, e_1^P, \theta_1^P \right)^T, \ldots, \left(r_M^P, e_M^P, \theta_M^P \right)^T \right)$$

$$Q_p = \left(\left(r_1^Q, e_1^Q, \theta_1^Q \right)^T, \ldots, \left(r_N^Q, e_N^Q, \theta_N^Q \right)^T \right)$$

r: distancia radial

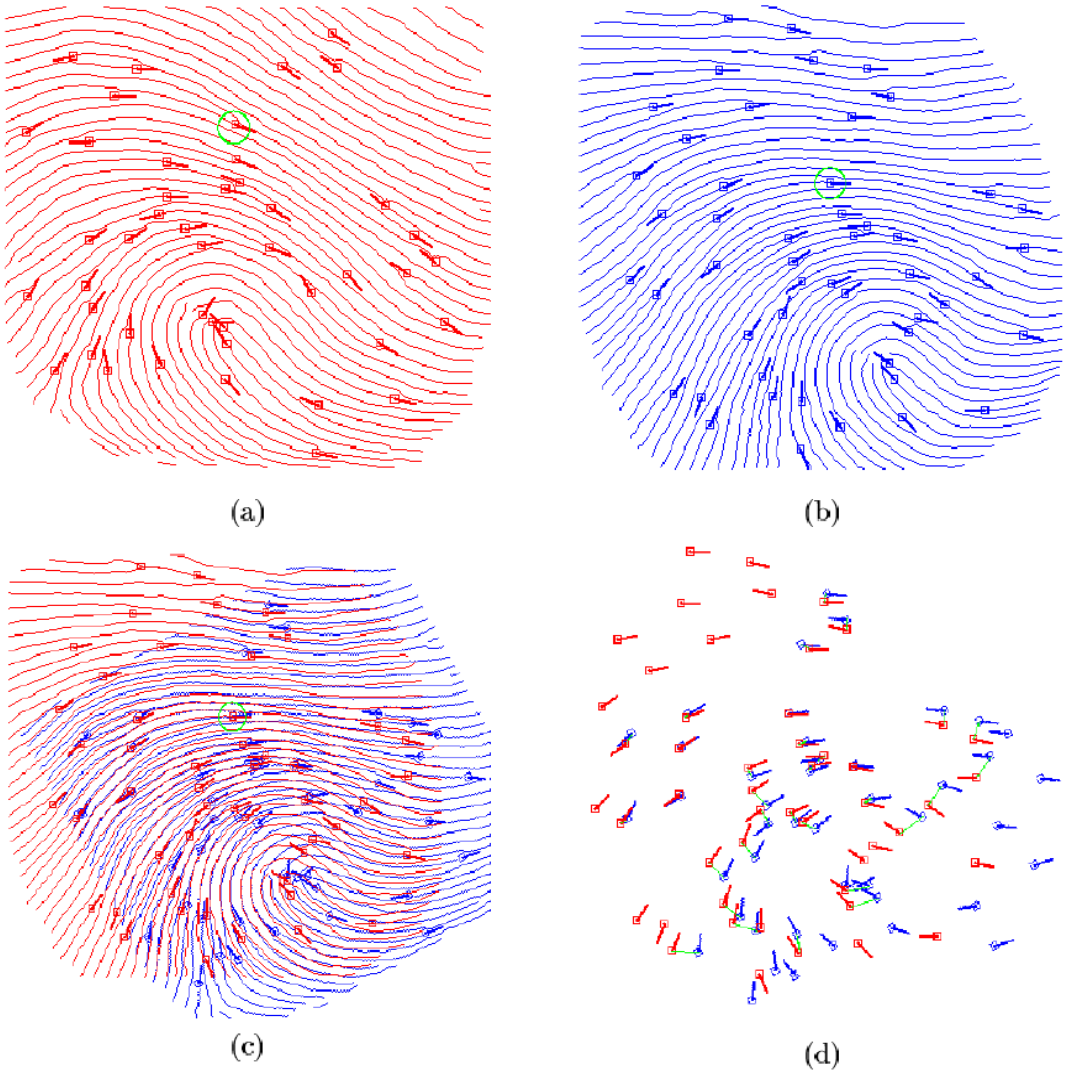
e: ángulo radial

θ: orientación respecto a la minucia de referencia



- Se aplica la distancia de disimilaridad entre las dos cadenas: muestra y patrón

Huella dactilar: técnica basada en minucias



Huella dactilar: dispositivos de captura

- Terminales completos de identificación por huella
- Lectores integrados (con software de soporte)
- Sensores:
  - Ópticos
    - V: Elevada resolución
    - D: Deformación no lineal del sensor
  - Estado sólido (sensores de tipo capacitivo, térmicos y piezoeléctricos)
    - V: Bajo consumo y reducido tamaño del dispositivo sensor
    - D: Elevada sensibilidad a variaciones de humedad de la huella
  - Ultrasónicos
    - V: Lectura tridimensional de la huella. Eliminación de ruido
    - D: Elevado precio y menor resolución que los sensores ópticos

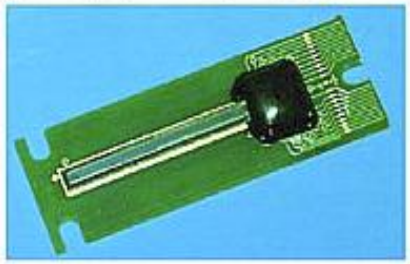
Importante: es recomendable que el área de la huella sea de 1 pulgada cuadrada y que la resolución de la imagen sea igual o superior a 500 dpi y 256 niveles de grises (100-500 Kbytes).

Huella dactilar: sensores

Secugen
http://www.secugen.com/

Digital Persona
http://www.digitalpersona.com

Veridicom
http://www.veridicom.com



Atmel
http://www.atmel.com

BMF
www.bm-f.com

FingerSec
www.fingersec.com

Huella dactilar: dispositivos de control de acceso

Carmen Sánchez Ávila

Huella dactilar: estado actual de la tecnología

- Ventajas:
  - Técnica muy desarrollada
  - Gran aceptación (para determinadas aplicaciones)
  - Sistemas de captura no invasivos y de bajo coste con posibilidad de incorporar fácilmente un sistema de detección de sujeto vivo
  - Facilidad de integración en diferentes entornos
  - Unicidad y estabilidad de la huella
- Desventajas:
  - Implicaciones policiales y judiciales
  - Necesidad de elevada calidad de la imagen digital
  - Necesidad de contacto físico con la superficie del sensor

- Resultados satisfactorios con los sistemas actuales (FVC- onGoing 2009):
  - **Green Bit S.p.A.**:
    - EER = 1,046%
    - FRR = 2,210% para FAR ≤ 0,1% y FRR = 3,152% para FAR ≤ 0,01%
    - Tiempo medio de verificación: 3 msg.
  - **Neurotechnology**:
    - EER = 1,528%
    - FRR = 3,043% para FAR ≤ 0,1% y FRR = 4,079% para FAR ≤ 0,01%
    - Tiempo medio de verificación: 3 msg.

Iris

Carmen Sánchez Ávila

Iris: principales características

- Potencialidad para la Identificación:
  - Mayor unicidad que la huella
  - Parámetros accesibles desde el exterior, a través de protección dada por la córnea
    - Textura del iris
    - Acceso visual a la retina a través de la pupila
  - Órgano estable (en muchos de sus parámetros):
    - Con la edad
    - Frente a accidentes (debido a la córnea)
  - Fácil detección de sujeto vivo
    - Por variaciones del tamaño de la pupila frente a cambios de iluminación
  - Manipulación compleja
    - Conllevaría potenciales riesgos en la visión del individuo
- Inconvenientes:
  - Utilización de elementos externos por parte de los usuarios

Iris: orígenes

- 1936: Frank Burch (oftalmólogo) proporciona la idea de que el iris se puede utilizar para identificar a una persona
- 1987: Leonard Flom y Aran Safir (oftalmólogos) patentan la idea de Burch
  - Contactan con **John G. Daugman** (profesor de la Universidad de Harvard) para que les desarrolle los algoritmos necesarios
- 1993: Publicación de parte de los algoritmos
  - J.G. Daugman, *"High Confidence Visual Recognition of Persons by a Test of Statistical Independence"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, n. 11, pp.: 1148-1161, 1993
- 1994: Patente de los algoritmos y fundación de IriScan Corp., empresa que se encargará de la explotación de las patentes. Se licencia la patente a diversas empresas, entre ellas Sensar Corp., NCR, Panasonic, etc.
- A partir del 2001, IriScan y Sensar deciden fusionarse creando la empresa **Iridian Technologies** (http://www.iridiantech.com/) que es la actual encargada de explotar las patentes

Iris: captura

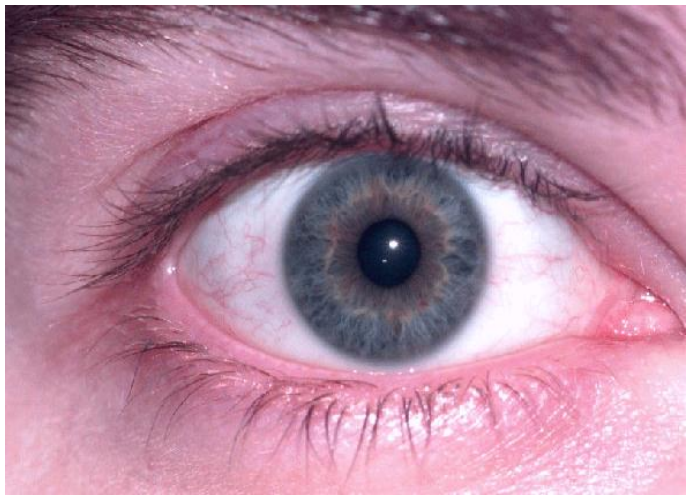
- La captura se realiza de forma no invasiva
  - Se realiza mediante una cámara digital o de video de alta resolución con un objetivo de aproximación, para enfocar en el ojo a una distancia del sujeto que no le resulte incómoda a éste
- Se requiere interacción por parte del usuario
  - Localización del ojo dentro de un campo de visión
  - En algunos sistemas se localiza el ojo en una escena y posteriormente se enfoca (de forma automática)
- Sin información de color
  - Luz infrarroja

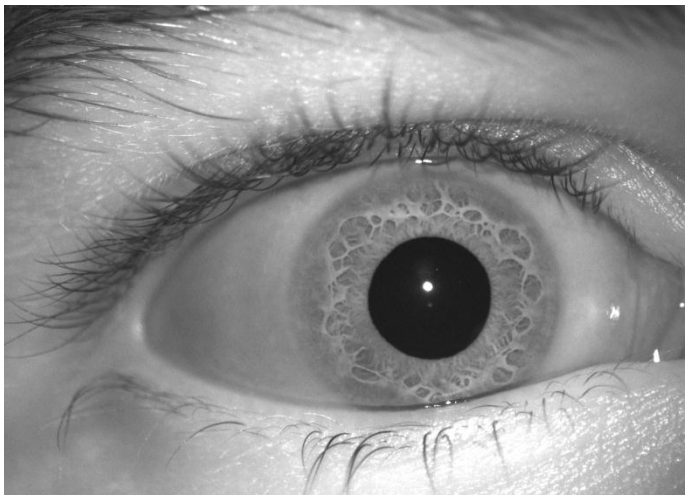
Iris: sistemas comerciales

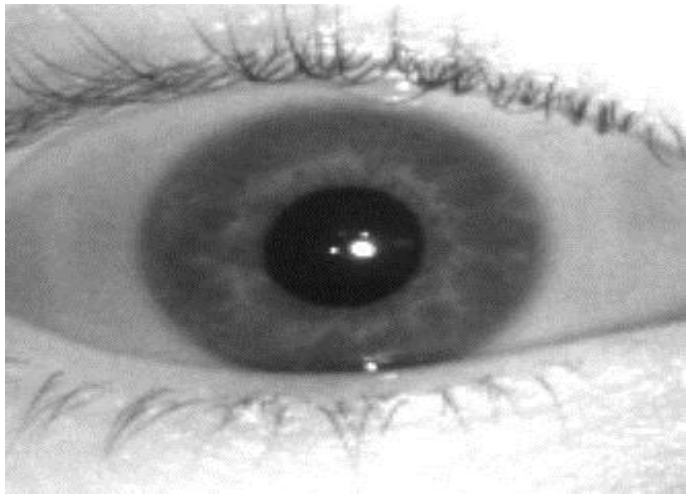
- Cámara de acceso físico:
  - LG
  - Panasonic
  - OKI
  - Senex
  - Evermedia
  - Jirix
- Cámara de PC:
  - Panasonic
- Cámara de Mano:
  - OKI (IrisPass-h)

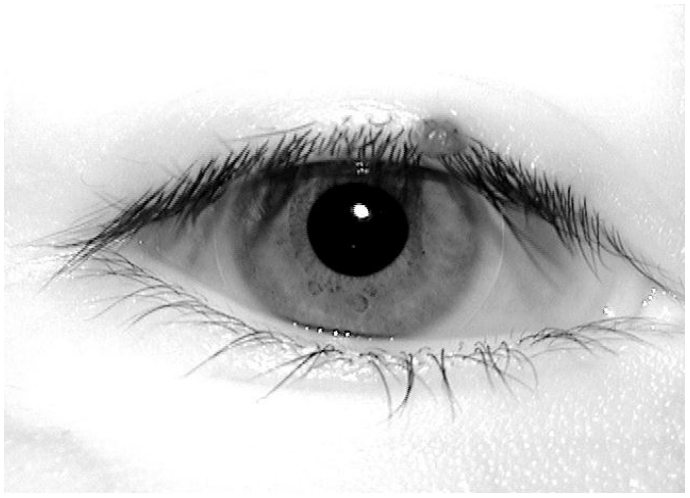
Carmen Sánchez Ávila

Iris: captura



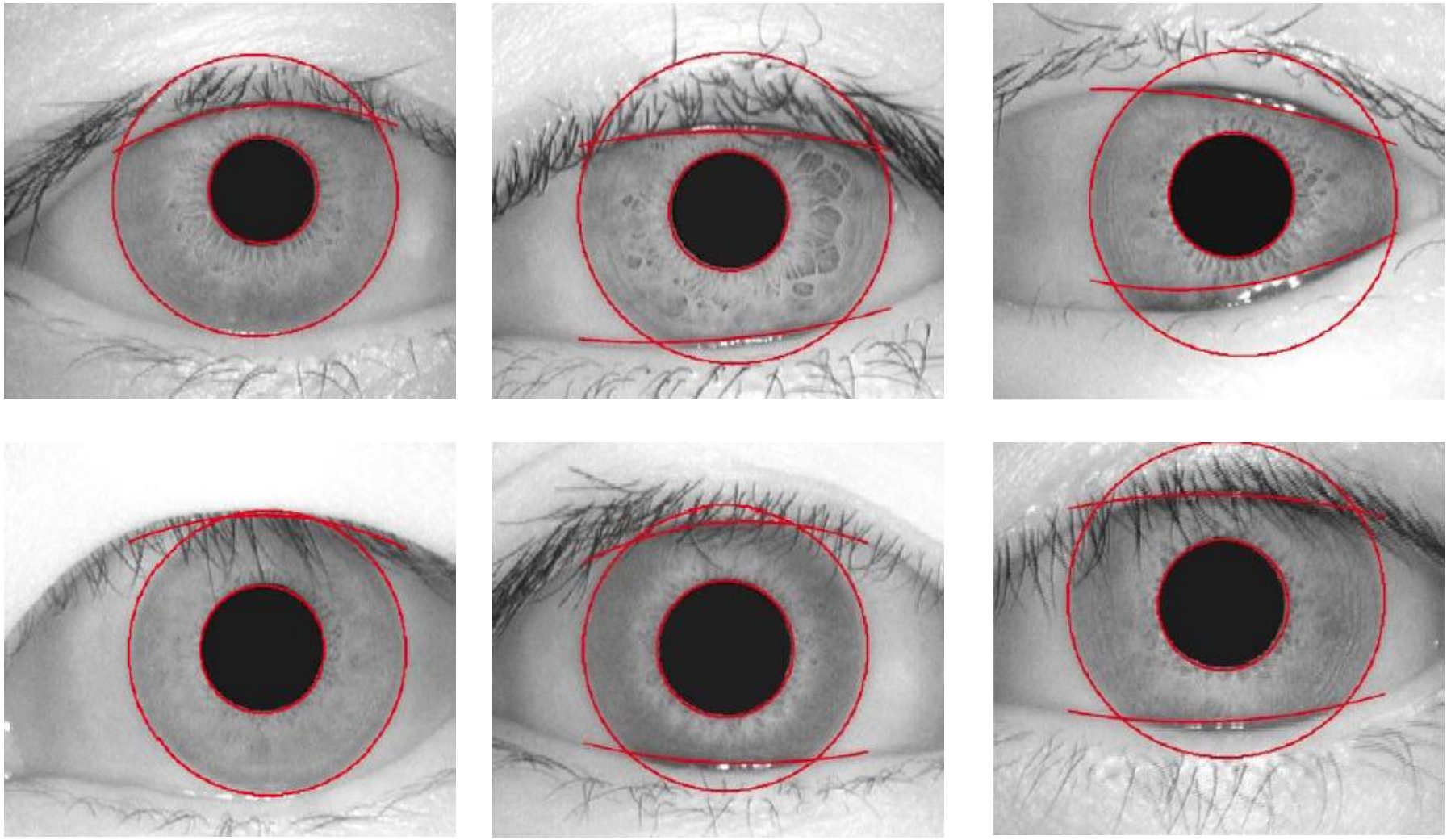






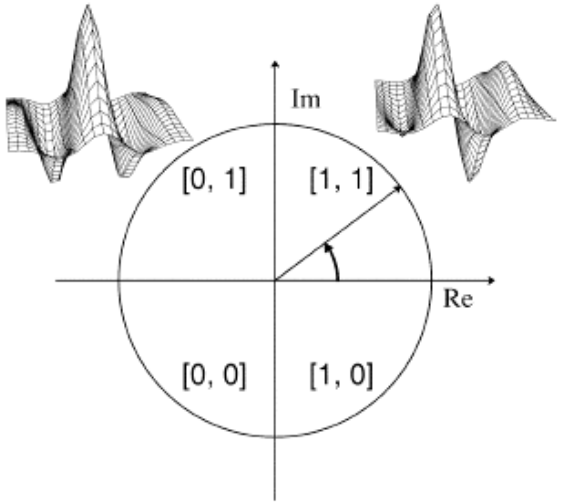
Carmen Sánchez Ávila

Iris: localización



Carmen Sánchez Ávila

Iris: extracción del patrón



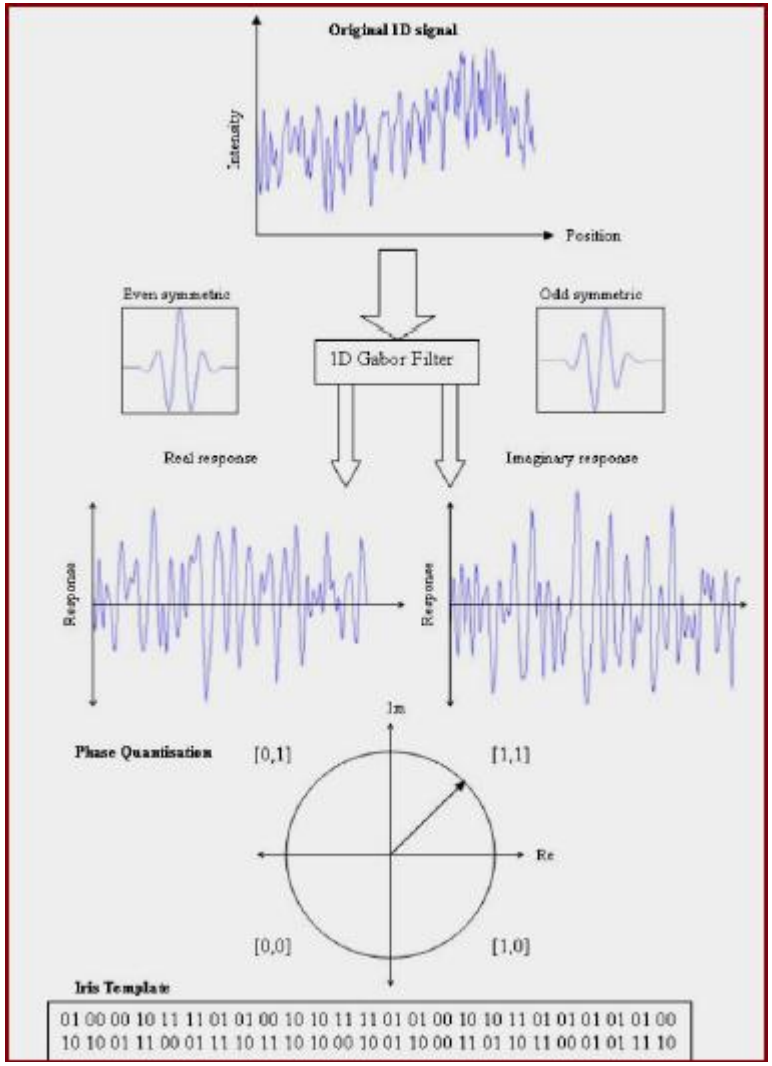
Filtros de Gabor en coordenadas polares

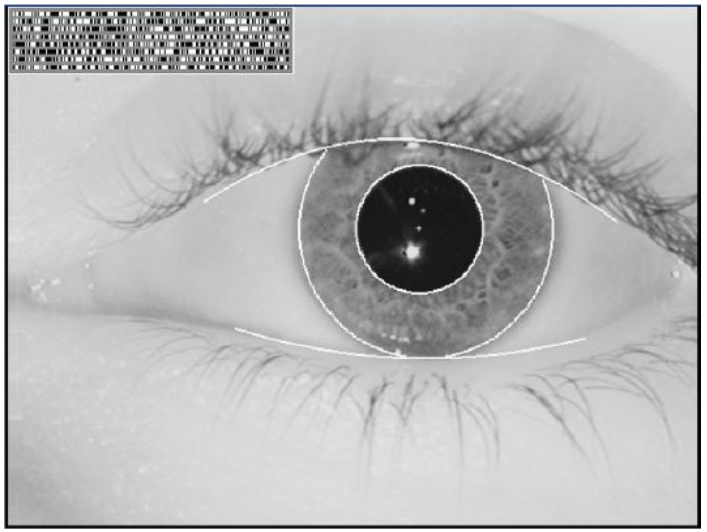
$$G(r,\theta) = e^{j\omega(\theta-\theta_0)}\, e^{-\frac{(r-r_0)^2}{\alpha^2}}\, e^{-j\frac{(\theta-\theta_0)^2}{\beta^2}}$$

Demodulación y cuantificación de la fase

$$g_{\{\mathrm{Re,Im}\}} = \mathrm{sgn}_{\{\mathrm{Re,Im}\}} \int_{\rho}\int_{\phi} I(\rho,\phi)\, e^{j\omega(\theta_0-\phi)}\, e^{-\frac{(r_0-\rho)^2}{\alpha^2}}\, e^{-j\frac{(\theta_0-\phi)^2}{\beta^2}}\, \rho\, d\rho\, d\phi$$

Iris: extracción del patrón





Patrón de iris (Iris Code)

2048 bits

(resumen la información de la textura del iris)

* John Daugman's personal website: http://www.cl.cam.ac.uk/users/jgd1000/

Iris: sistemas actuales

Aeropuerto de Frankfurt

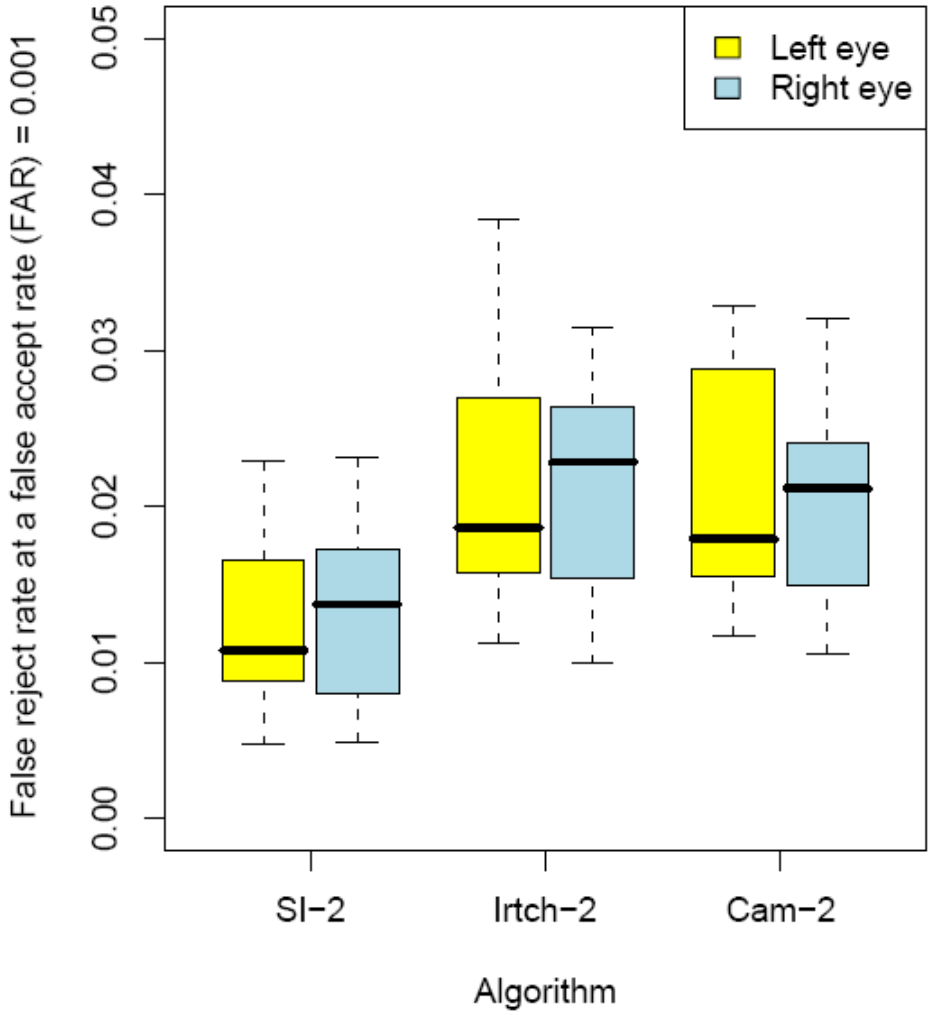
Aeropuerto de Schiphol

Tokyo

Emiratos árabes

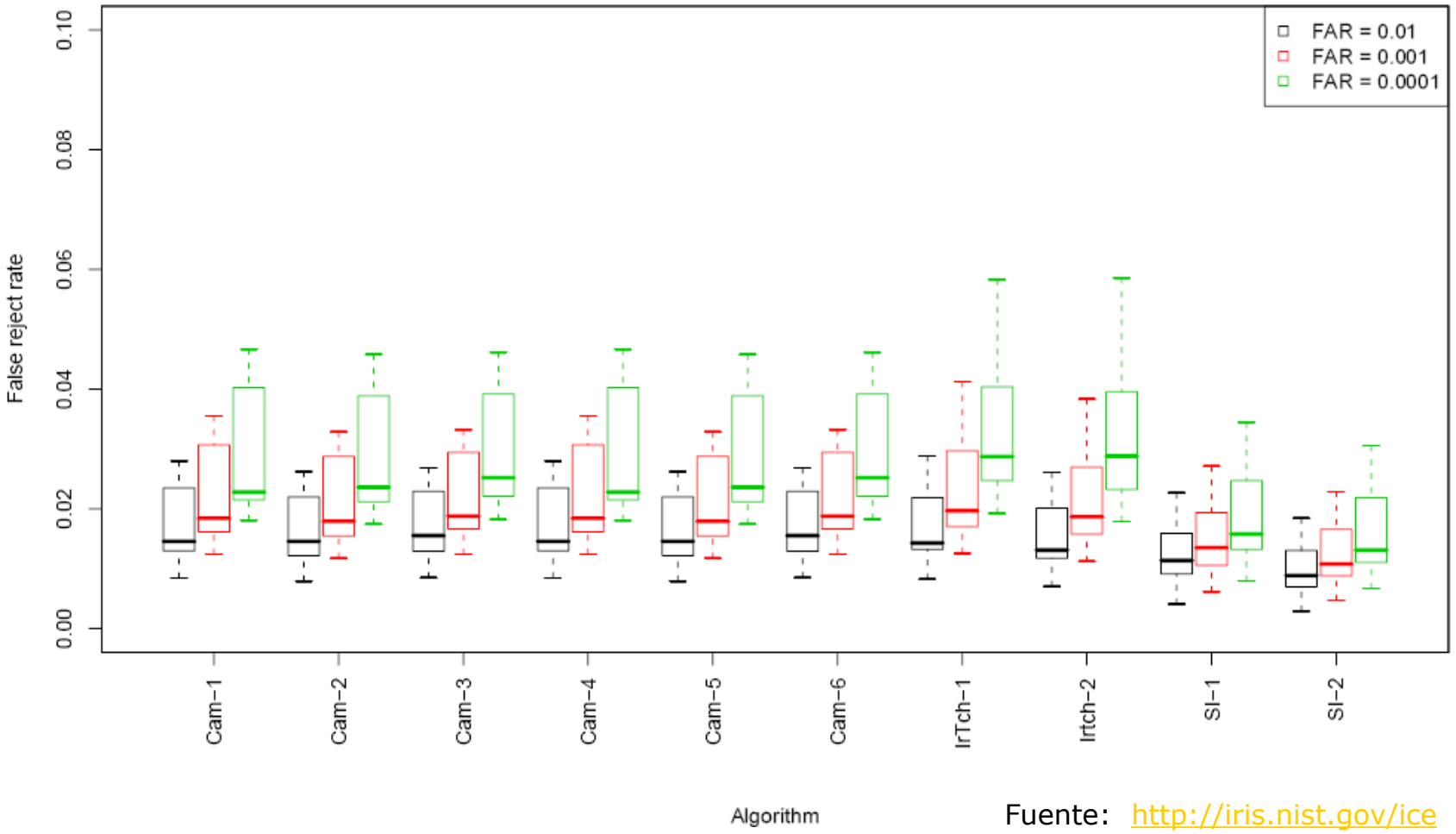
Carmen Sánchez Ávila

Iris: rendimiento de los sistemas



Fuente:
http://iris.nist.gov/ice

Iris: rendimiento de los sistemas



Fuente: http://iris.nist.gov/ice

Características de la mano

Carmen Sánchez Ávila

Mano: características principales

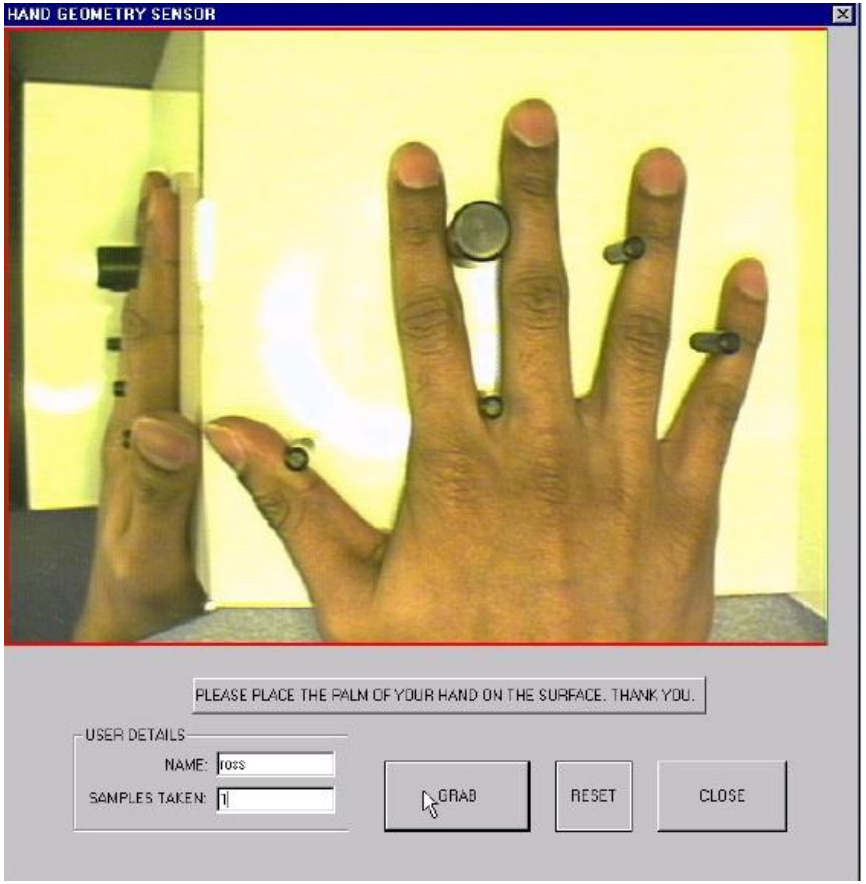
- Unicidad: media. No existen estudios detallados que demuestre su unicidad.

  En el sector: correcta
- Estabilidad: media, ya que los cambios de peso de una persona pueden modificar la geometría de la mano.

  Solución: tomar medidas relativas
- Coste: bajo. Sólo se precisa una cámara de media/baja calidad y una plataforma diseñada al efecto
- Aceptabilidad: muy alta (no tiene implicaciones legales y es muy fácil de usar)
- Tamaño del patrón: muy pequeño (decenas de bytes)

Mano: dispositivos de captura

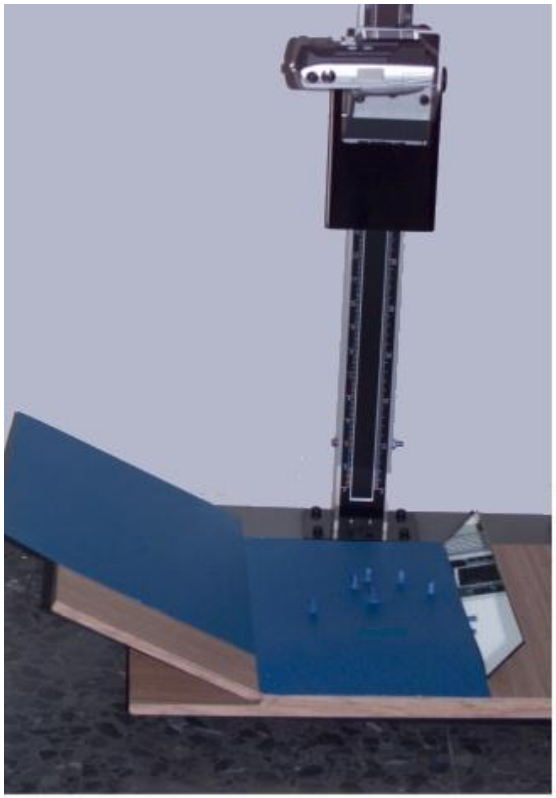
Mano: extracción del patrón



a) El sistema toma 3muestras de la silueta de la mano

b) Forma un patrón de 9 bytes tomando el promedio de las 3 muestras

Mano: extracción del patrón



a)

b)

c)

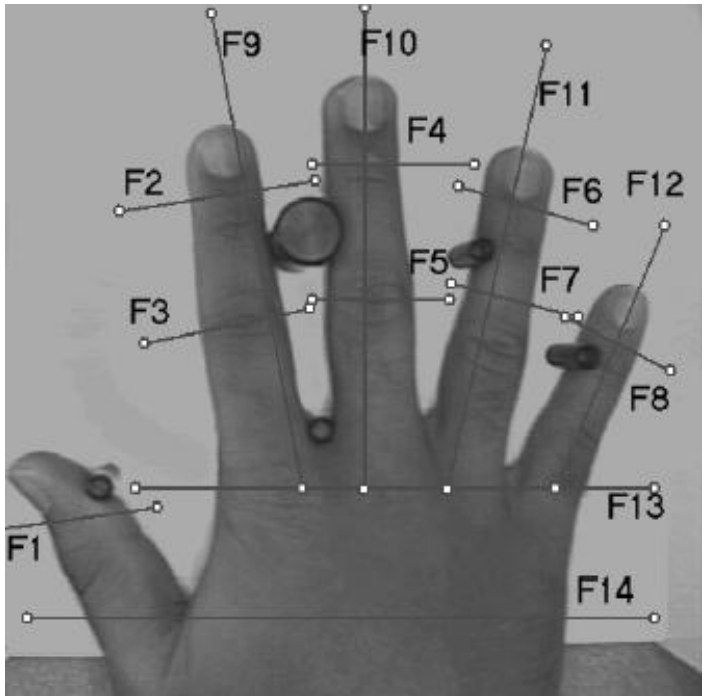
a) Plataforma con 6 topes y espejo colocado 60 º sobre la superficie

b) Colocación de la mano

c) Imagen obtenida de 640x480 y 256 colores

Mano: extracción del patrón

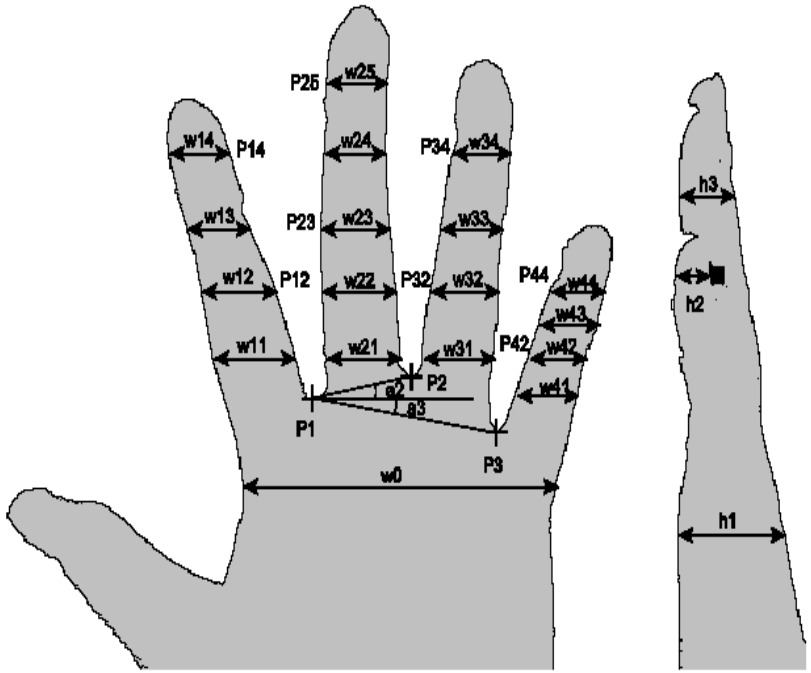
MSU



Características: algunas anchuras interdedo, dedos y mano

Medida de disimilaridad: distancia euclídea

GUTI-GBTNI

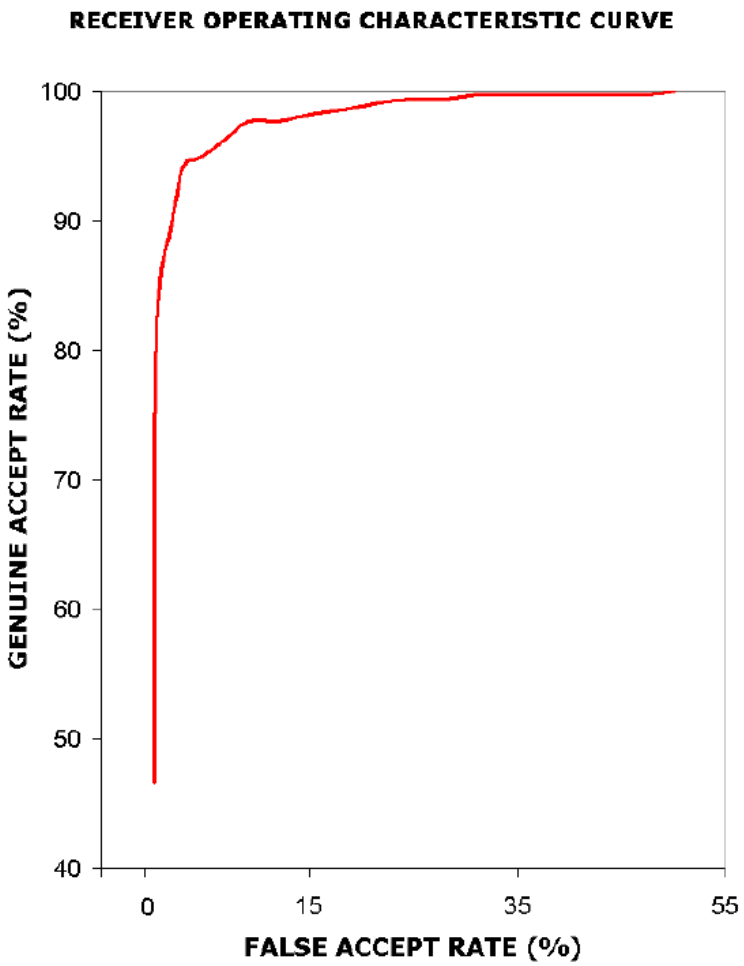


Características: anchuras interdedo, dedos y mano, desviaciones y alturas

Medida de disimilaridad: GMM's

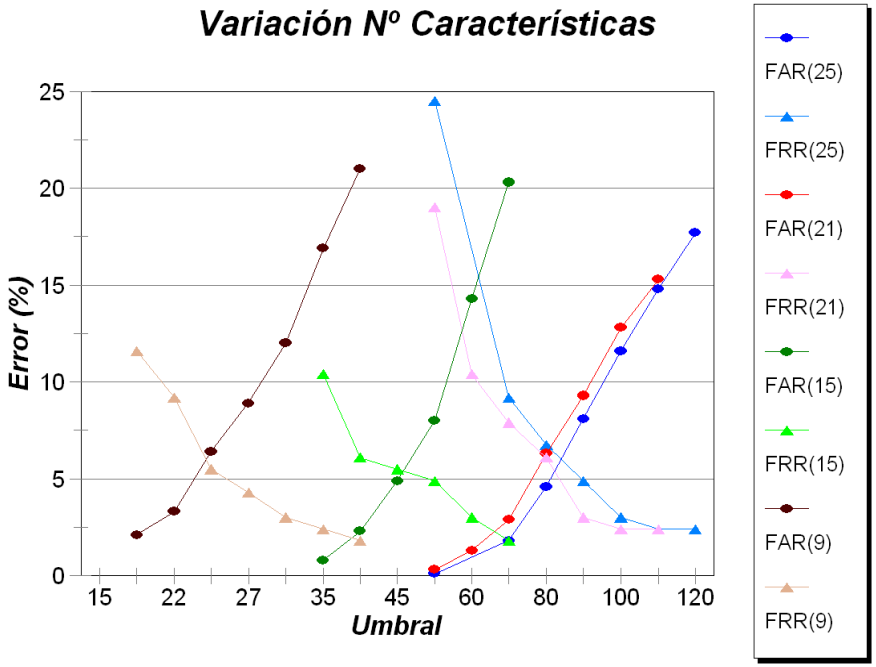
Mano: algunos resultados

MSU



GUTI-GBTNI

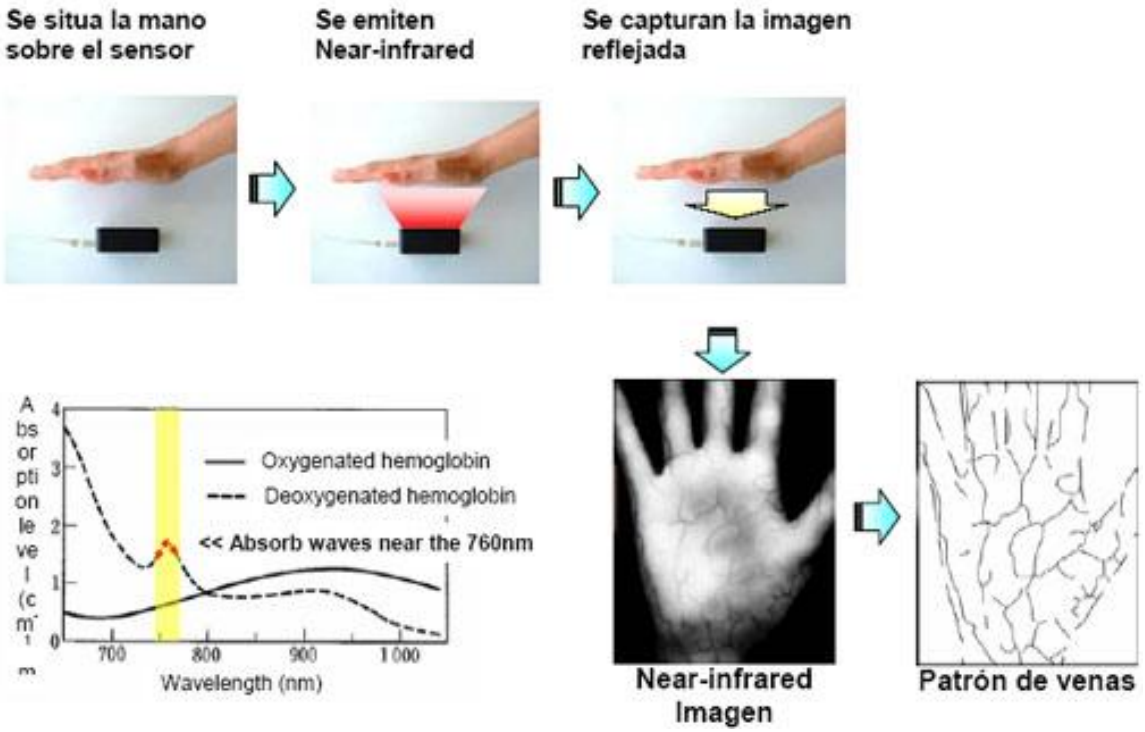
Nº Características	GMMs
25	96 %
21	97 %
15	96 %



Carmen Sánchez Ávila

Mano: imagen vascular de la palma

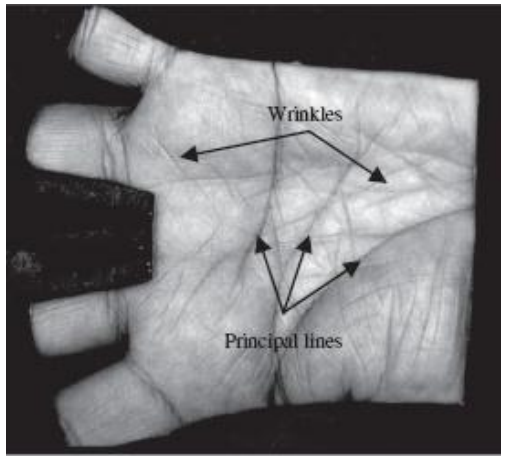
Sistema Palm Secure (Fujitsu)



Carmen Sánchez Ávila

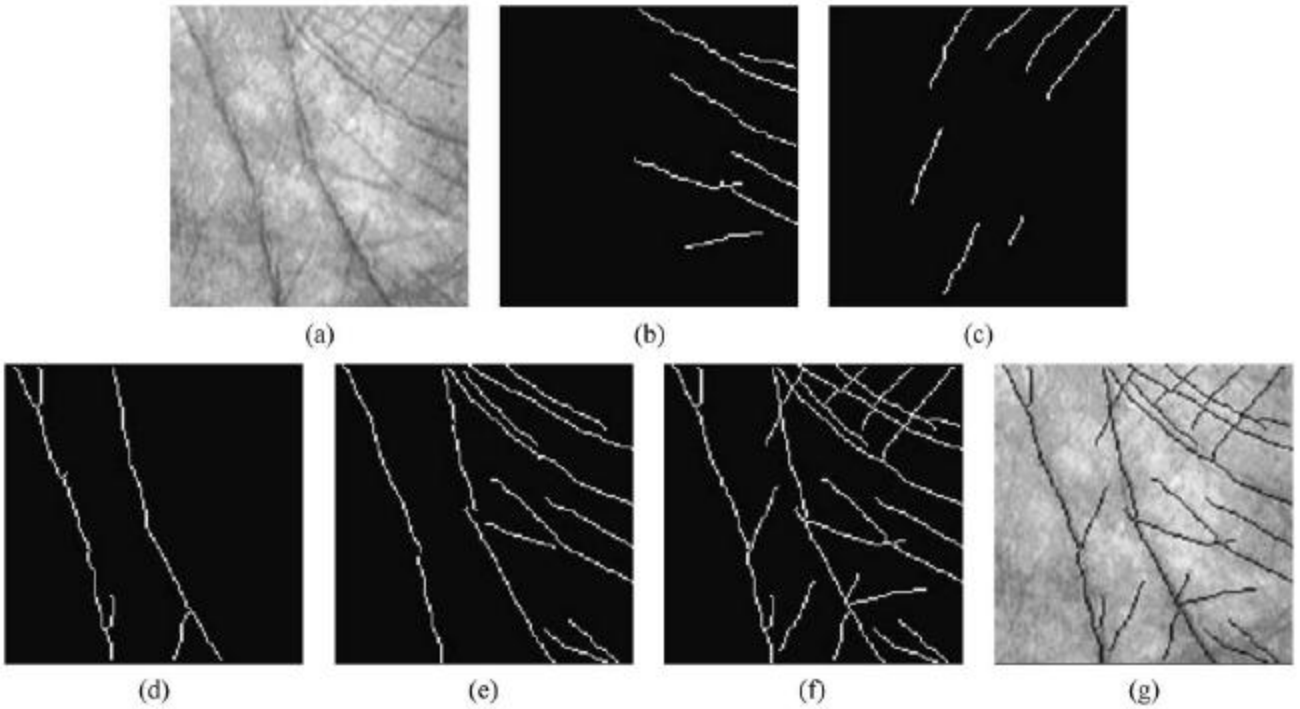
Mano: región palmar

Región palmar



Captura y pre-procesado

Mano: región palmar



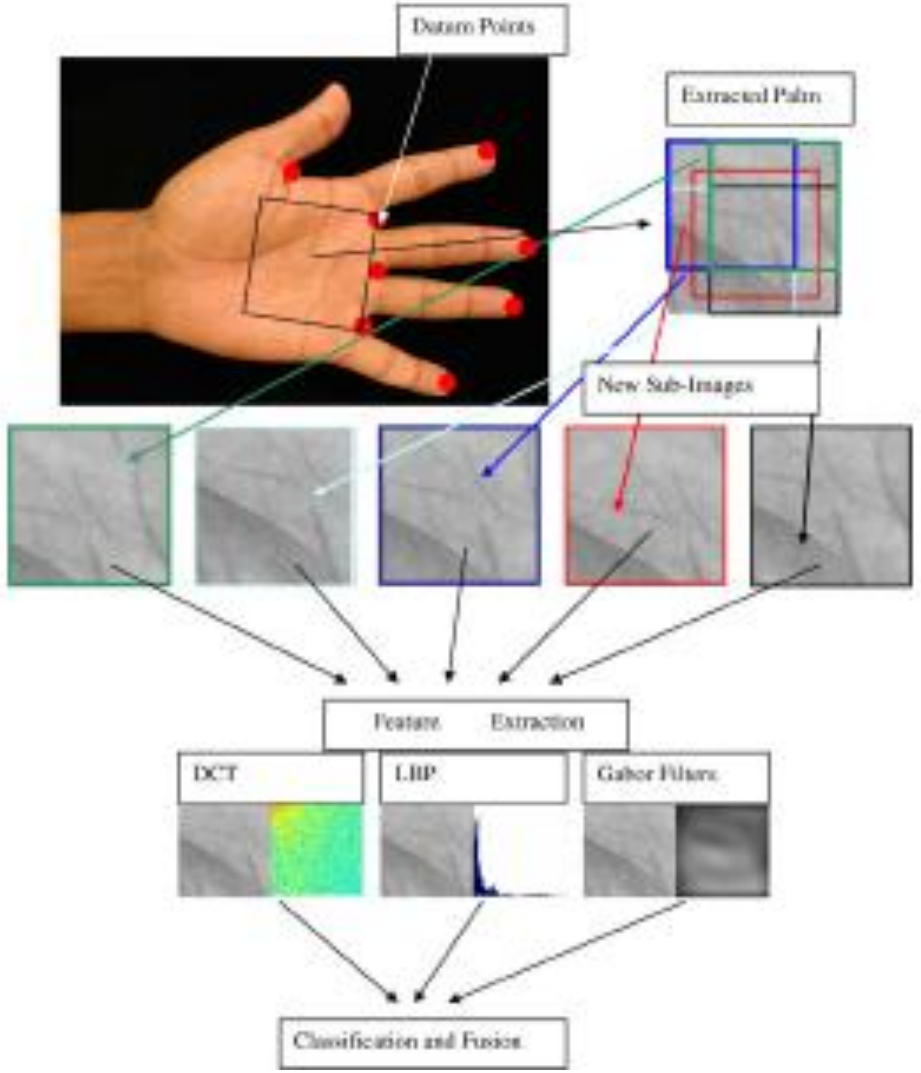
Proceso de extracción de las líneas de la palma de la mano

Mano: región palmar

Algoritmos de verificación

- Aproximaciones basadas en líneas
  - Operadores de detección de bordes (Canny, Sobel, etc)
  - Algoritmos de comparación (distancia euclídea, HMM's, distancia de Haussdorf, redes neuronales, etc.)
- Aproximaciones basadas en subespacios
  - Extracción de características: filtros de Gabor, DCT, wavelets, etc.
  - Proyección en subespacios (LDA, PCA, ICA, etc.)
- Aproximaciones estadísticas
  - Estadísticos locales (Gabor, wavelets, etc y media, varianzas locales)
  - Estadísticos globales (momentos, centros de gravedad, etc.. calculados directamente sobre la imagen completa)
- Otras aproximaciones
  - Métodos de codificación basados en orientación (CompCode, POC, RLOC, BOCV, etc)
  - ..

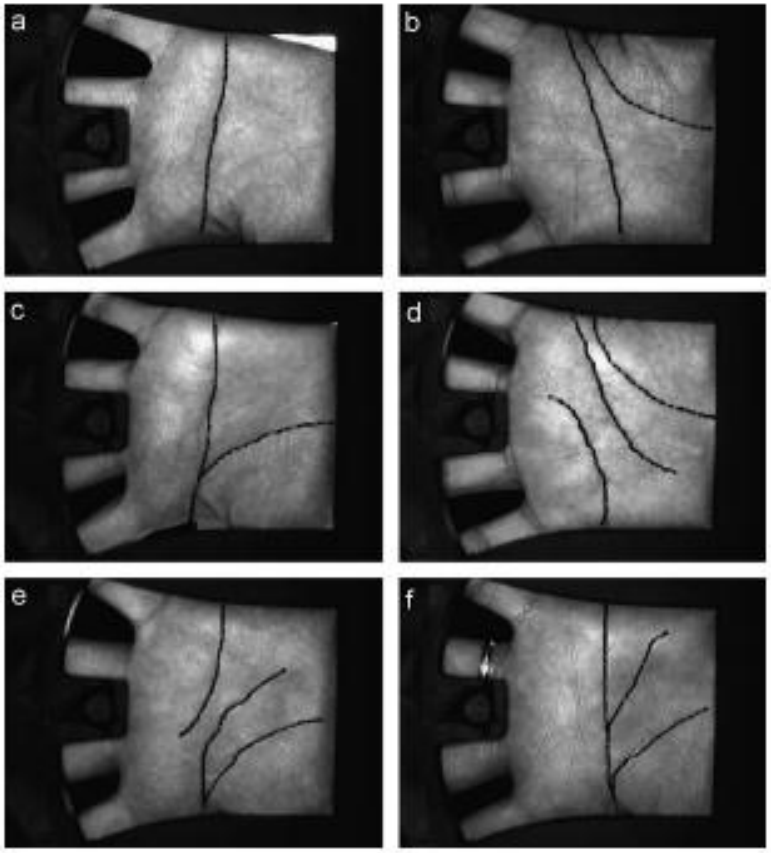
Mano: región palmar



Carmen Sánchez Ávila

Mano: región palmar

Identificación



Tipos de regiones palmar: primera aproximación

Carmen Sánchez Ávila

Mano: región palmar

Algunos resultados en Verificación

	PalmCode	FusionCode	Competive Code	RLOC
FAR (%)	4×10^{-5}	4×10^{-5}	4×10^{-5}	4×10^{-5}
FRR (%)	17.2	12.1	4.86	1.631
EER (%)	0.98	0.82	0.47	0.16

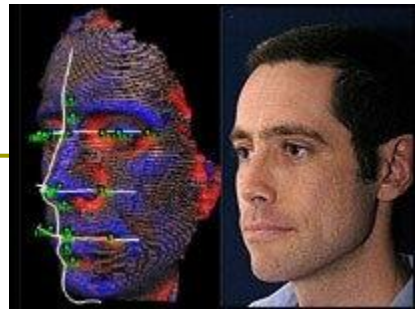
Operation	Method	Execution time (ms)
Preprocessing		316
Feature extraction	RLOC	70
	Competitive Code	220
Matching	RLOC	3.9

Fuente: W. Jiaa, *D.-S. Huanga, D. Zhang,* Palmprint verification based on robust line orientation code, Pattern Recognition 41 (2008) 1504 – 1513.

Características faciales

Carmen Sánchez Ávila

Características faciales



Propiedades principales

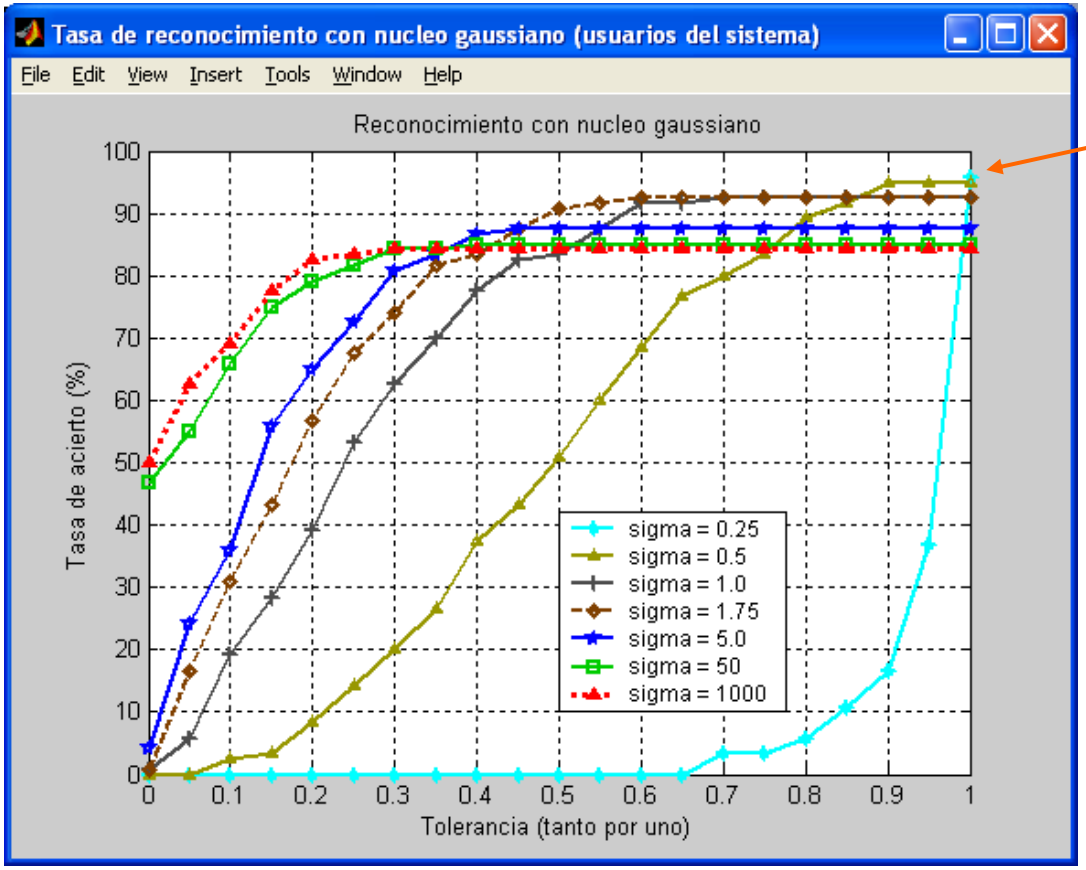
- Unicidad: media. No existen estudios detallados que demuestre su unicidad
- Estabilidad: media, ya que influyen muchos factores: cambios en iluminación, pose, etc.
- Coste: bajo. Sólo se precisa una cámara de captura y una plataforma diseñada al efecto
- Aceptabilidad: alta (no tiene implicaciones legales, es fácil de usar y no es invasivo
- Tamaño del patrón: medio (dependiendo del método utilizado)
- Fiabilidad: media

Características faciales: algunos métodos 2D

- Redes neuronales
  - Técnicas de backpropagation
  - Más indicadas para detección y localización de caras en imágenes, no para identificación
- Análisis de la geometría facial
  - Localización de las diferentes características
  - Distancias entre ellas
  - Geometría de las mismas
- Comparación de grafos
  - Construccción de un grafo alrededor de la cara
  - Localización de las características de la misma
  - Inclusión de otros datos (color de la piel, textura)
- Autocaras
  - Teoría de la Información
  - Extrae componentes discriminantes de la identidad
- Fisherface
  - Utiliza información intra-clase para maximizar la separación entre clases

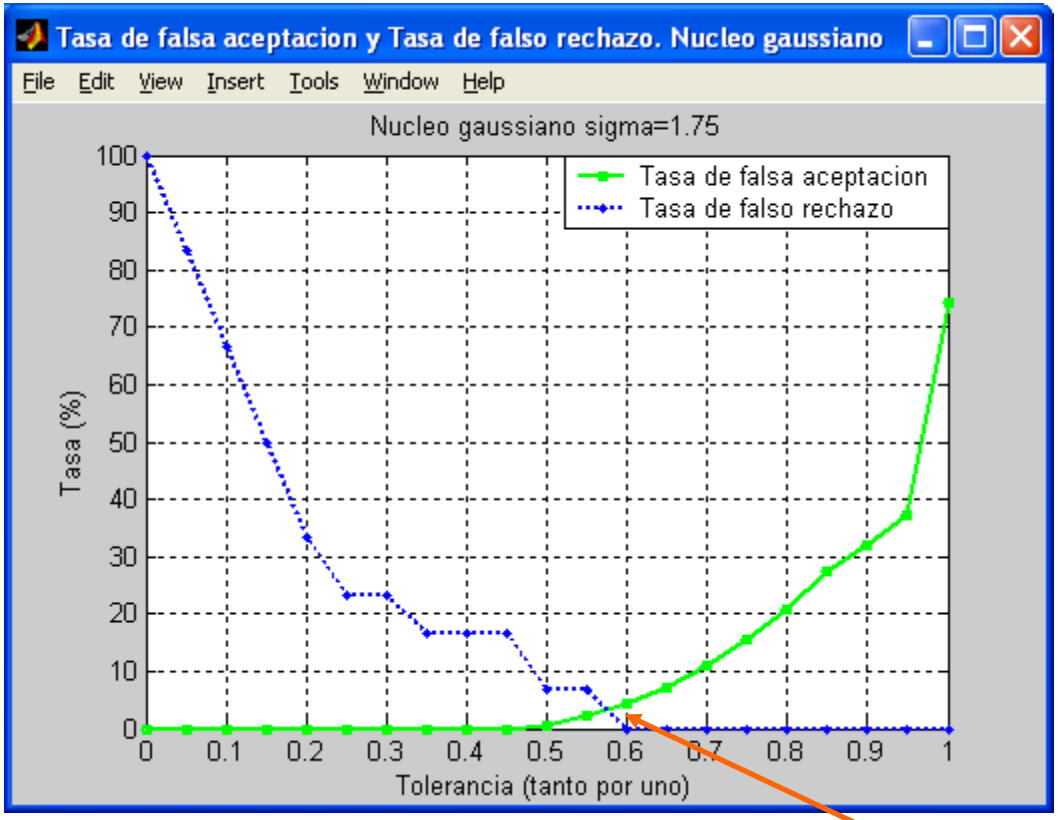
Características faciales: algunos resultados

- Resultados en identificación con PCA y SVM (núcleo gaussiano)



Características faciales: algunos resultados

- Resultados en autenticación con PCA y SVM (núcleo gaussiano)



EER = 3,76 %

Características faciales: algunos sistemas comerciales

- Cognitec
  - FaceVACS Entry – Access Control
- A4Vision
  - Vision Access – 3D Face Reader
- Viisage
  - Face PASS
- Dreams MIRH
  - MIRH Eye ACS
- Identix
  - FaceIt Argus
  - ABIS
- Geometrix
  - FaceVision 3D

http://www.frvt.org/

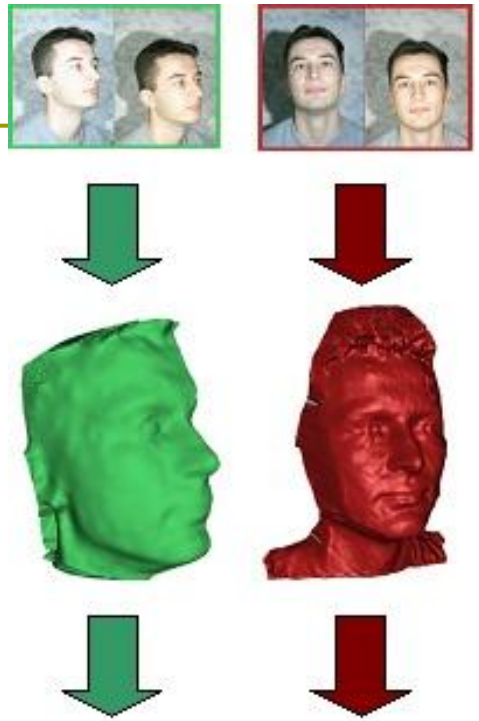
Características faciales: algunas desventajas

- No es tan fiable como otro tipo de característica biométrica
- Requiere alta capacidad de almacenamiento
- Se precisan imágenes de buena calidad

Problemas:

- Iluminación
  - Los cambios de iluminación afectan al rendimiento del sistema
  - Saturación de la imagen
- Poses y expresiones
  - Diferencias en la orientación de la cabeza y las diferentes expresiones
- Calidad de imagen
  - Las cámaras actuales (CCTV, etc.) no ofrecen a menudo la calidad necesaria

Características faciales: sistemas 3D

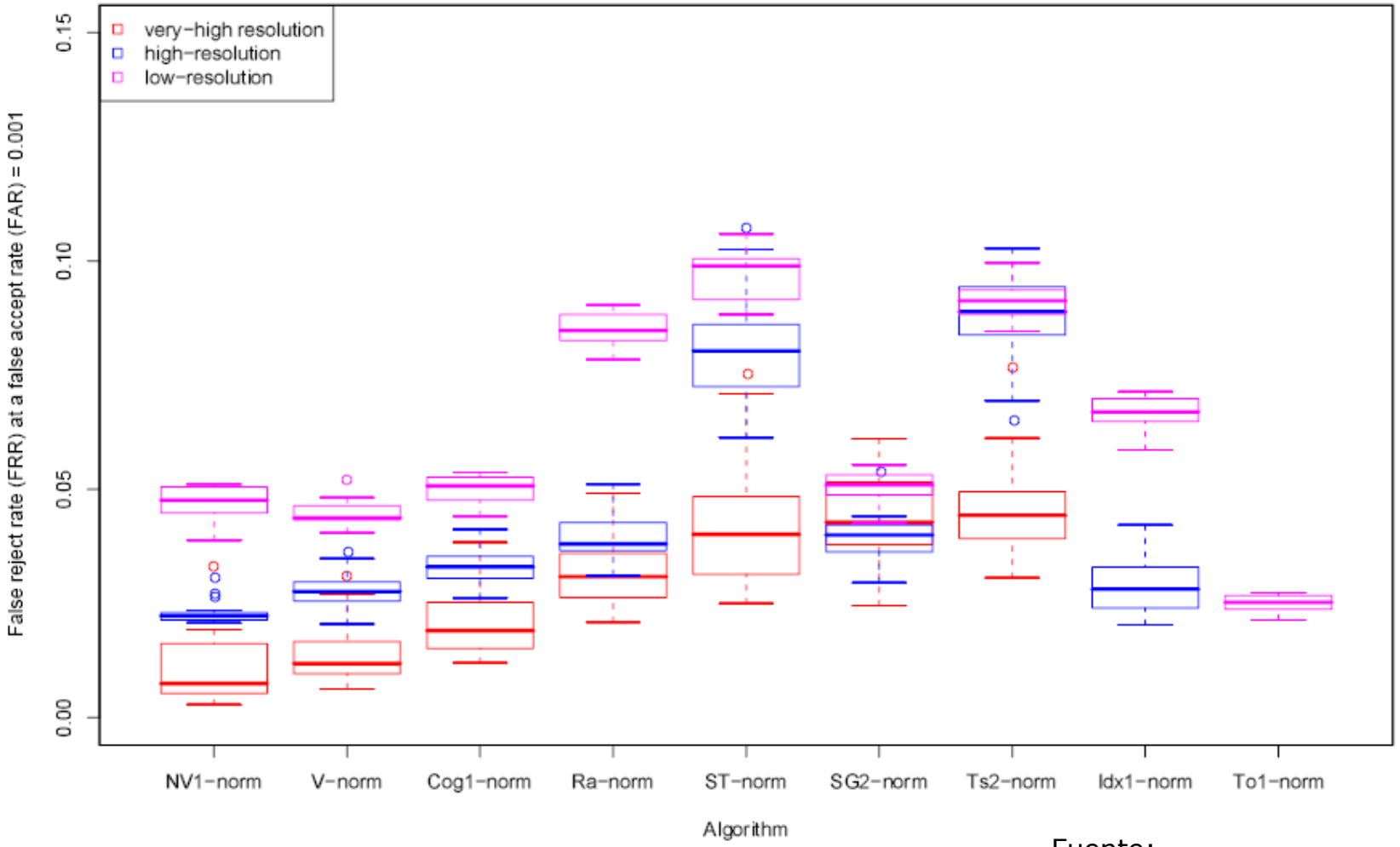


Una alternativa: reconocimiento facial 3D

- Ventajas:
  - Incrementa la fiabilidad del sistema
  - Elimina los problemas de iluminación y poses
  - Posee suficiente información invariante frente a cambios en la expresión, utilización de gafas, etc.
- Paradigmas:
  - Comparación de perfiles
  - Modelos 3D basados en firmas de puntos
  - Comparación mediante segmentación de la superficie
  - AURA (Advanced Uncertain Reasoning Architecture)

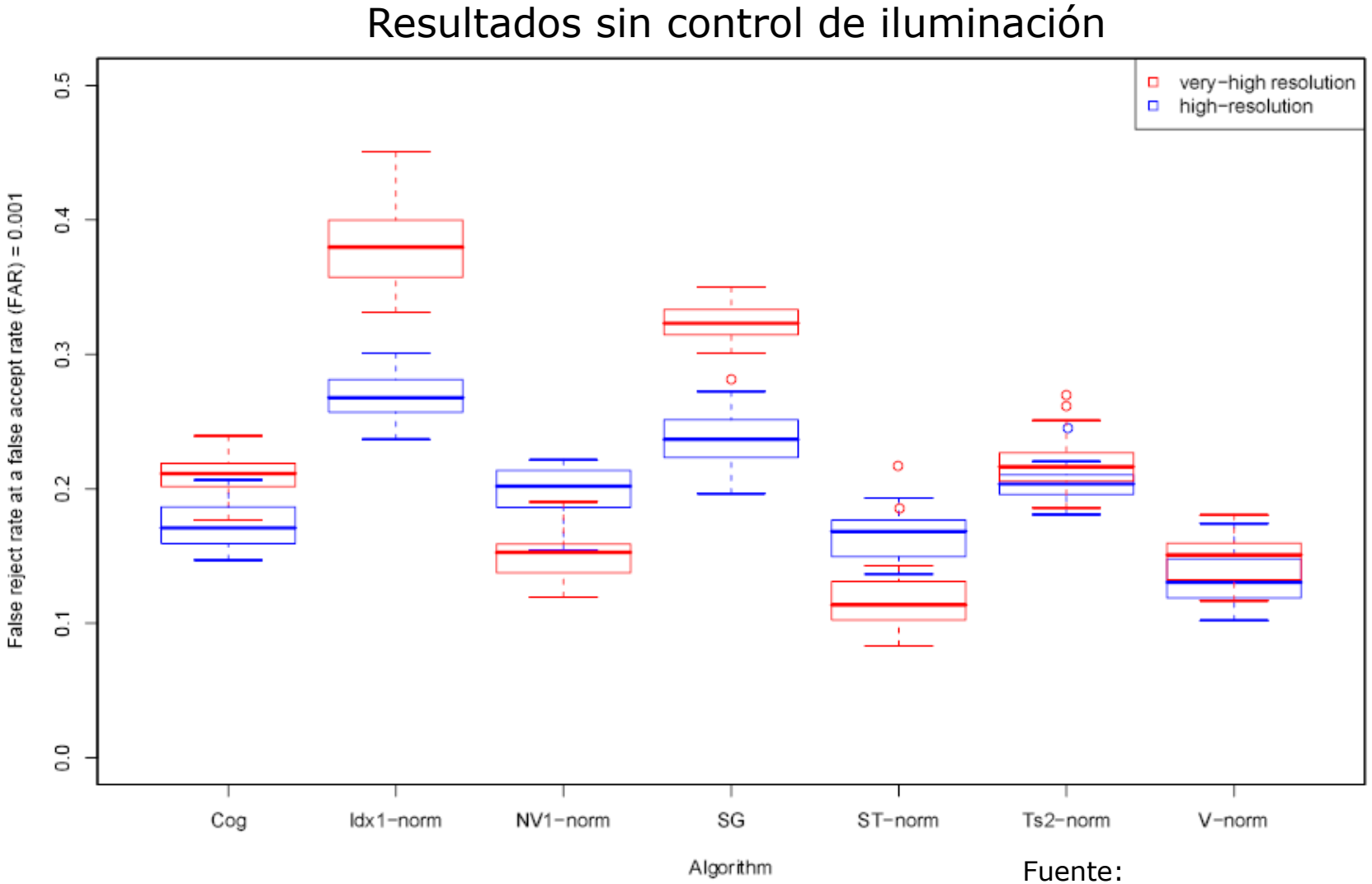
Características faciales: resultados

Resultados con control de iluminación



Fuente:
http://iris.nist.gov/ice

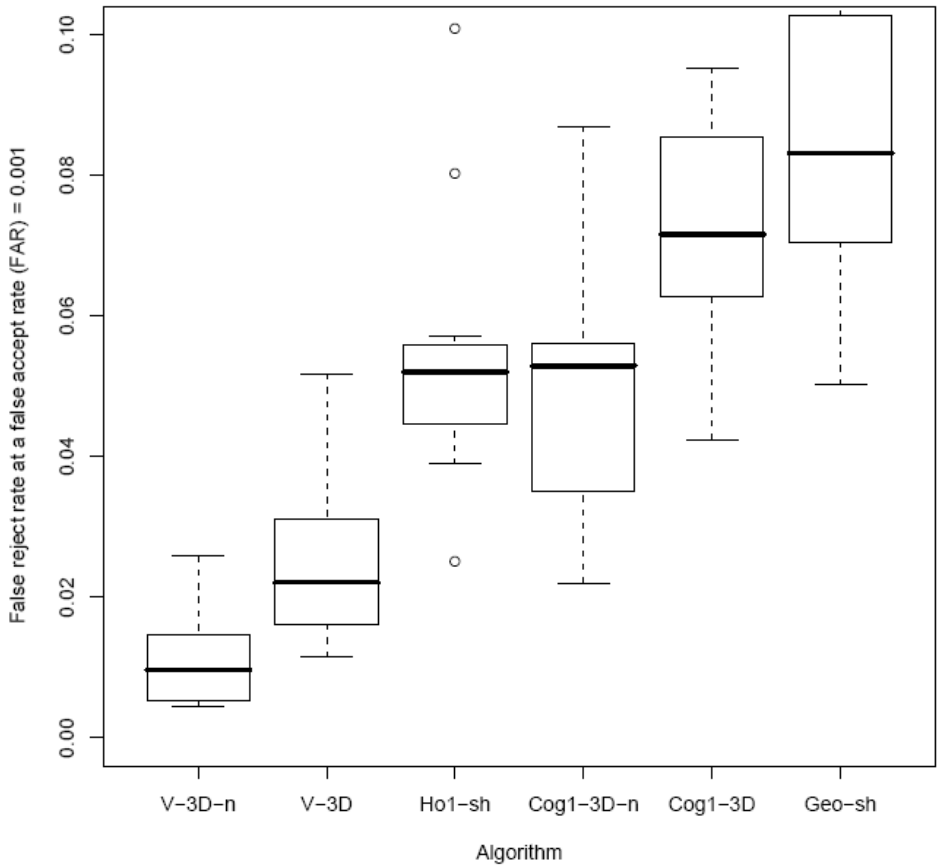
Características faciales: resultados



Fuente: http://iris.nist.gov/ice

Características faciales: resultados

Resumen de resultados para algoritmos de reconocimiento facial 3D



Fuente:
http://iris.nist.gov/ice

Algunas aplicaciones de la Biometría

Carmen Sánchez Ávila

Algunas aplicaciones de la Biometría

Podemos dividirlas en tres grandes grupos:

- Comerciales
  - Control de acceso físico o lógico (edificios, ordenadores, telefonos, PDAs, etc)
  - Comercio electrónico
  - ATMs
  - Gestión de historiales médicos
- Gubernamentales
  - Tarjeta de identificación nacional
  - Carnet de conducir
  - Tarjetas de seguridad social
  - Control de Pasaportes
- Forenses
  - Investigaciones policiales
  - Identificación de terroristas
  - Identificación de personas desaparecidas

Algunas aplicaciones de la Biometría: sistemas actuales







Carmen Sánchez Ávila

Tendencias futuras en Biometría

Carmen Sánchez Ávila

Biometría multimodal

Tasas de error en Biometría unimodal

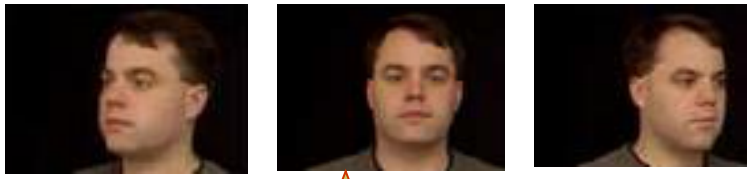
	FRR	FAR
Huella	2%	0,1%
Iris	0,03%	0,001%
Cara	0,5%	0,001%
Mano	3%	3%
Voz	10-20%	2-5%

En una instalación con 200.000 usuarios diarios, tendríamos:

- 4.000 usuarios erróneamente rechazados al día si utilizaran identificación por huella, 60 si se utiliza iris, 1.000 si se utiliza cara, 6.000 si utiliza mano y 30.000 (aprox.) si utilizan sólo voz.
- 200 usuarios erróneamente aceptados con huella, 2 con iris, 2 con cara, 6.000 con mano y 7000 (aprox.) con voz.

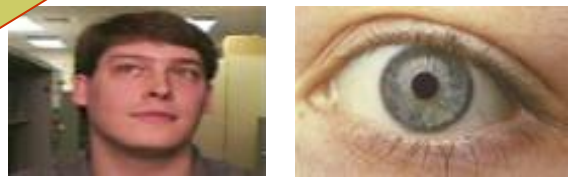
Biometría multimodal: posibilidades

Múltiples capturas (1)



Múltiples sensores (2)

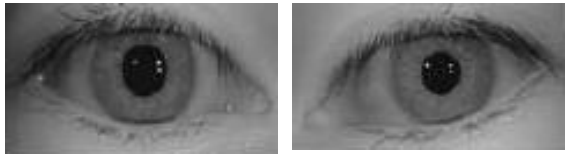
Múltiples características (5)



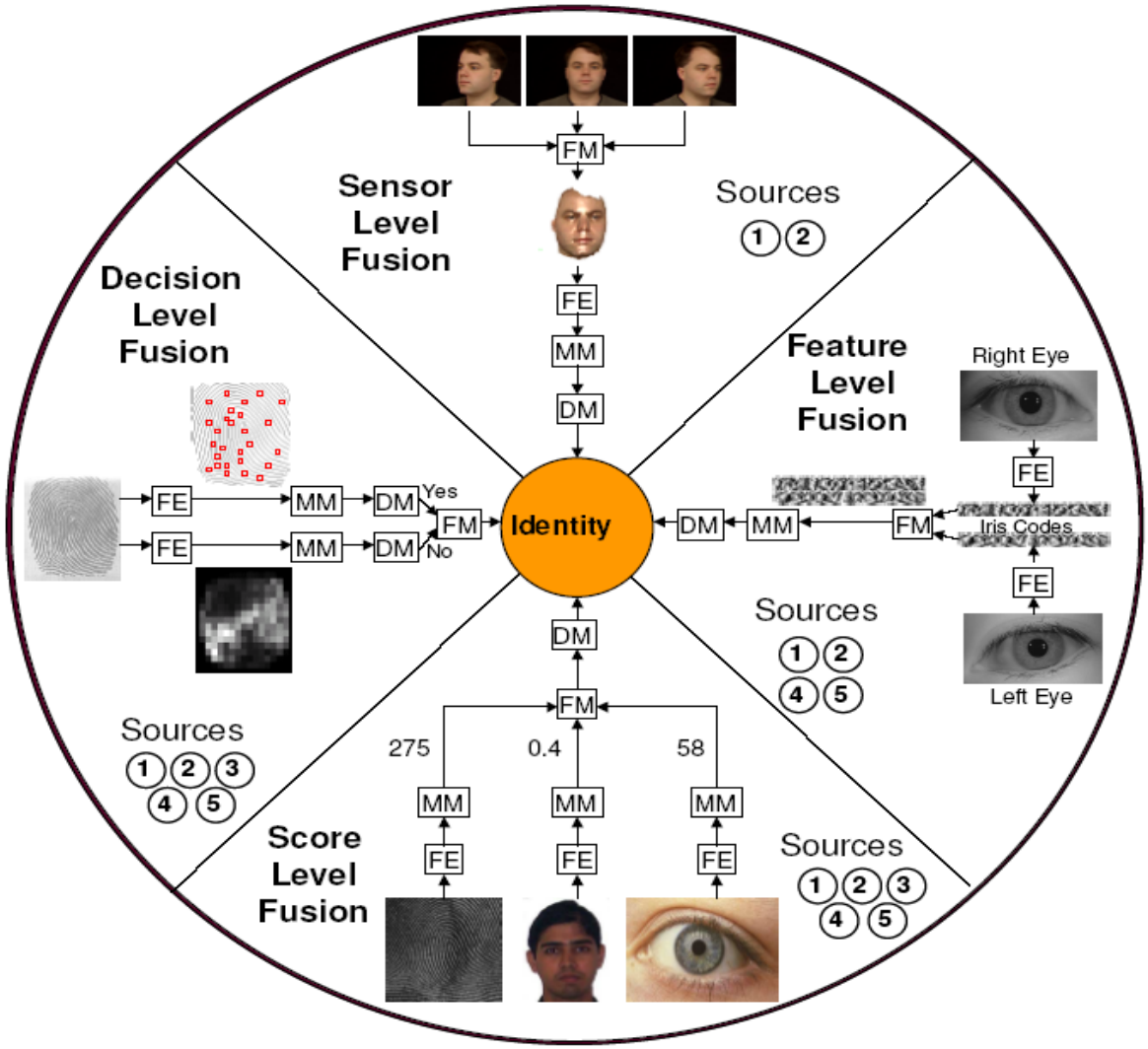
Sistemas multimodales

Múltiples representaciones (3)

Múltiples unidades (4)



Biometría multimodal: niveles de fusión



Carmen Sánchez Ávila

Otras líneas futuras de trabajo

- Sistemas Match-on-Card
  - Combinación de las tecnologías biométricas y de tarjeta inteligente
  - Proceso de comparación dentro de la tarjeta
  - El patrón no "viaja" fuera de la tarjeta en la que se almacena de forma segura
- Cripto-Biometría
  - Combinación de la Criptografía y la Biometría
  - Implementación de sistemas Cripto-Biométricos de clave pública
  - Patrón biométrico como clave privada

Bibliografía

- A. K. Jain, R. Bolle and S. Pankanti (eds.), Biometrics: Personal Identification in a Networked Society, Kluwer Academic Press, 1999.
- J. L. Wayman, A. K. Jain, D. Maltoni and D. Maio (eds.), Biometric Systems. Technology, Design and Performance Evaluation, Springer, 2005.
- M. Tapiador y J. A. Sigüenza (coord.), Técnicas biométricas aplicadas a la seguridad, Ra-Ma, 2005.
- S. Z. Li and A. K. Jain (eds.), Handbook of Face Recognition, Springer, 2005.
- D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2005.
- A.K. Jain, P. Flynn, A. Ross (eds.), Handbook of Biometrics, Springer, 2008.

- Enlaces de interés:
  - http://www.biometrics.org/
  - http://www.eubiometricforum.com/
  - http://www.bioapi.org/